PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-092040
(43)Date of publication of application : 31.03.2000

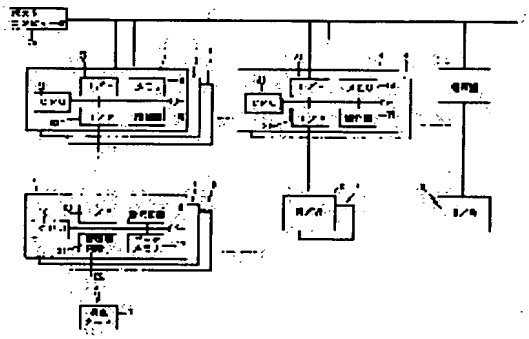
(51)Int.Cl. H04L 9/10
B42D 15/10
G06K 17/00
G07B 15/00
H04L 9/14
H04L 9/32

(21)Application number : 10-258016
(22)Date of filing : 11.09.1998

(71)Applicant : OMRON CORP
(72)Inventor : WAKABAYASHI NAOYUKI

(54) STORAGE MEDIUM, READER/WRITER, CARD SYSTEM, METHOD FOR USING CRYPTOGRAPHIC KEY, STATION SERVICE SYSTEM, AND CARD ISSUING MACHINE

(57)Abstract:
PROBLEM TO BE SOLVED: To update a cryptographic key as required, e.g. periodically or in case of possibility of a decoded cryptographic key without using all cryptographic keys at random by updating the cryptographic key selected by a command sent from a reader/writer.
SOLUTION: A reader/writer 6 stores old cryptographic keys that were used in the past and not in use at present and a cryptographic key that is currently in use. Furthermore, the reader/writer 6 transmits an update command to a passenger card 7 to allow the passenger card 7 to update its cryptographic key from an older cryptographic key to the cryptographic key used at present when the cryptographic key used by the passenger card 7 is the cryptographic key that was used in the past but not in use at present according to a response from the passenger card 7 as a result of communciation between the reader/ writer 6 and the passenger card 7, and the passenger card 7 updates the cryptographic key into the cryptographic key used at present in response to the command. Thus, the cryptographic key of the old passenger card 7 having been issued before is finally updated into the cryptographic key used at present.



LEGAL STATUS

[Date of request for examination]	03.09.1999
[Date of sending the examiner's decision of rejection]	08.08.2000
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	3553387
[Date of registration]	14.05.2004

[Number of appeal against examiner's decision of rejection]	2000-14400
[Date of requesting appeal against examiner's decision of rejection]	08.09.2000
[Date of extinction of right]	

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.

2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1] The storage characterized by to provide a cryptographic key storage means memorize two or more cryptographic keys, a cryptographic key selection means choose either from from among two or more cryptographic keys memorized by said cryptographic key storage means, and a renewal means of a cryptographic key update said cryptographic key choose with the command sent out from aforementioned read-out / write-in machine, in the storage constituted so that authentication and a communication link may perform between read-out / write-in machine using a cryptographic key.
[Claim 2] The storage characterized by rewriting some [at least] cryptographic keys of two or more cryptographic keys memorized by said cryptographic key storage means from read-out / write-in machine in claim 1.
[Claim 3] In read-out / write-in machine constituted so that authentication and a communication link might be performed between storages using a cryptographic key A cryptographic key storage means to memorize two or more cryptographic keys, and a cryptographic key selection means to choose either from from among two or more cryptographic keys memorized by said cryptographic key storage means, A cryptographic key learning means to get to know whether the cryptographic key this storage is carrying out [the cryptographic key] current use by the response from said storage is a cryptographic key used in the past with read-out / the write-in machine concerned, At the time of the cryptographic key for which the cryptographic key said storage is carrying out [the cryptographic key] current use was used in the past, they are read-out / write-in machine characterized by providing a renewal command sending-out means of a cryptographic key to send out the command which updates the cryptographic key of said storage.
[Claim 4] Read-out / write-in machine characterized by providing a cryptographic key modification means to change the cryptographic key which read-out / the write-in machine concerned use with the command from a high order device in claim 3.
[Claim 5] Read-out / write-in machine characterized by rewriting some [at least] cryptographic keys of two or more cryptographic keys which said storage has memorized in claim 3.
[Claim 6] a storage according to claim 1 or 2 -- a card -- carrying out -- this card, and claim 3 thru/or 5 -- the card system with which a card, and read-out / write-in machine are characterized by to perform mutual recognition using the updated cryptographic key after updating the cryptographic key of a card at the time of the cryptographic key for which the cryptographic key has read-out / write-in machine of a publication in either, and the card is carrying out [the cryptographic key] current use was used in the past with aforementioned read-out / write-in machine.
[Claim 7] A storage, and each read-out / write-in opportunity are made to memorize two or more cryptographic keys. Read-out / write-in machine The encryption data based on the cryptographic key which this storage transmitted from the storage is using, It judges whether the cryptographic key which compares the encryption data created by the cryptographic key which read-out / write-in machine is using, and the storage, and read-out / write-in machine are using is in agreement. Said encryption data transmitted from the storage when not in agreement, The cryptographic key compares the encryption data created by the cryptographic key used in the past with read-out / write-in machine, and the storage is carrying out [the cryptographic key] current use When it is the cryptographic key which judged whether it was the cryptographic key used in the past, and was used for said past It is the cryptographic key operation characterized by transmitting the updating command which makes the cryptographic key which

this storage is using update to a storage, and for a storage answering said updating command, and updating a cryptographic key.
[Claim 8] A storage according to claim 1 or 2 is used as an entrainment card. This entrainment card, It has the automatic ticket gate equipped with read-out / write-in machine according to claim 3 or 4 which performs read-out/writing to this. Read-out / write-in machine The encryption data based on the cryptographic key which this entrainment card transmitted from the entrainment card is using, It judges whether the cryptographic key which compares the encryption data created by the cryptographic key which read-out / write-in machine is using, and the entrainment card, and read-out / write-in machine are using is in agreement. Said encryption data transmitted from the entrainment card when not in agreement, The cryptographic key which compares the encryption data created by the cryptographic key used in the past with read-out / write-in machine, and the entrainment card is using When it is the cryptographic key which judged whether it was the cryptographic key used in the past, and was used in the past It is the station service system characterized by transmitting the updating command which makes the cryptographic key which this entrainment card is using update to an entrainment card, and for an entrainment card answering said updating command, and updating a cryptographic key.
[Claim 9] It is the station service system which uses a storage according to claim 1 or 2 as an entrainment card, has this entrainment card and the card issue machine equipped with read-out / write-in machine according to claim 5 which performs read-out/writing to this, and is characterized by read-out / write-in machine rewriting two or more cryptographic keys memorized by this entrainment card at the time of issue of an entrainment card.
[Claim 10] The card issue machine which uses a storage according to claim 1 or 2 as an entrainment card, sets as it so that said cryptographic key which carries out current use may be chosen with a cryptographic key selection means, and publishes this entrainment card for it while writing two or more cryptographic keys which are due to be used the cryptographic key which carries out current use, and in the future in the cryptographic key storage means of this entrainment card.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.

2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention] This invention relates to a card issue machine at station service system lists, such as a storage which memorizes data, read-out / write-in machine which performs read-out/writing to this storage, a card system using them, suitable cryptographic key operation for them, and an automatic wicket using them.
[0002]
[Description of the Prior Art] For example, when processing the card which is a storage for the close payment of a card etc. with read-out / write-in machine of an automatic tariff collection machine, it is necessary to secure the security nature of a card. Therefore, encryption of the mutual recognition using a code or a communication link is usually performed between the card, and read-out / write-in machine. In addition, although mutual recognition is attesting mutually whether read-out / write-in machine which serves as a communications partner, in view of a card side being just, and whether the card which is a communications partner, in view of a read-out side / write-in machine side being just, a partner usually judges by whether the just cryptographic key is known mutually.
[0003]
[Problem(s) to be Solved by the Invention] In above-mentioned cipher processing, although there is a method with which all cards, and read-out / write-in machines also used the same cryptographic key (common cryptographic key), when a common cryptographic key is known by others, by this method, there is once a fault that the security nature of the whole system will be spoiled.
[0004] In order to abolish this fault, two or more cryptographic keys which two or more cryptographic keys are stored in a card, and a card has also in read-out / write-in machine are made to memorize, and there is a system it was made to have security nature raised by using any one cryptographic key in said two or more cryptographic keys at random in cipher processing between cards in write-in read-out / machine side.
[0005] When considering as the problem in such a case has the danger that two or more cryptographic keys of all will be monitored and decoded while using the cryptographic key for said random and a card, and read-out / write-in machine communicate by non-contact especially, the danger increases. Then, although it can consider making two or more cryptographic keys of all that a card memorizes change into two or more of other cryptographic keys all at once, modification of such a cryptographic key is considered from the use gestalt of the card that many cards are used being published, and is impossible in practice.
[0006] In view of an above-mentioned technical technical problem, it succeeds in this invention, and not all cryptographic keys are used for it at random, but when required, when there is a possibility that the cryptographic key might be decoded, it enables it to update a cryptographic key, and, moreover, it aims at periodical or being made not to change two or more cryptographic keys of a storage all at once.
[0007]
[Means for Solving the Problem] In order to attain the above-mentioned purpose, it constitutes from this invention as follows.
[0008] Namely, the storage of this invention of claim 1 is set to the storage constituted so that authentication and a communication link might be performed between read-out / write-in machine using a cryptographic key. A cryptographic key storage means to memorize two or more cryptographic keys, a

cryptographic key selection means to choose either from from among two or more cryptographic keys memorized by said cryptographic key storage means, and a renewal means of a cryptographic key to update said cryptographic key to choose with the command sent out from aforementioned read-out / write-in machine are provided.

[0009] Here, updating means switching and using the cryptographic key currently used for another cryptographic key of two or more cryptographic keys, and it will be used at every updating for the cryptographic key which was being used till then by one cryptographic key in two or more cryptographic keys, replacing with.

[0010] Moreover, the communication link between a storage, and read-out / write-in machine may be which method of a wired system or radio system.

[0011] The storage of this invention of claim 2 rewrites some [at least] cryptographic keys of two or more cryptographic keys memorized by said cryptographic key storage means from read-out / write-in machine in claim 1.

[0012] In read-out / write-in machine constituted so that read-out / write-in machine of this invention of claim 3 might perform authentication and a communication link between storages using a cryptographic key A cryptographic key storage means to memorize two or more cryptographic keys, and a cryptographic key selection means to choose either from from among two or more cryptographic keys memorized by said cryptographic key storage means, A cryptographic key learning means to get to know whether the cryptographic key this storage is carrying out [the cryptographic key] current use by the response from said storage is a cryptographic key used in the past with read-out / the write-in machine concerned, At the time of the cryptographic key for which the cryptographic key said storage is carrying out [the cryptographic key] current use was used in the past, a renewal command sending-out means of a cryptographic key to send out the command which updates the cryptographic key of said storage is provided.

[0013] Read-out / write-in machine of this invention of claim 4 possess a cryptographic key modification means to change the cryptographic key which read-out / the write-in machine concerned use with the command from a high order device, in claim 3.

[0014] Read-out / write-in machine of this invention of claim 5 rewrite some [at least] cryptographic keys of two or more cryptographic keys which said storage has memorized in claim 3.

[0015] The card system of this invention of claim 6 uses a storage according to claim 1 or 2 as a card. This card, claim 3 thru/or 5 -- it has read-out / write-in machine of a publication in either, and at the time of the cryptographic key for which the cryptographic key the card is carrying out [the cryptographic key] current use was used in the past with read-out / write-in machine, after updating the cryptographic key of a card, a card, and read-out / write-in machine perform mutual recognition using the updated cryptographic key.

[0016] The cryptographic key operation of this invention of claim 7 makes a storage, and each read-out / write-in opportunity memorize two or more cryptographic keys. Read-out / write-in machine The encryption data based on the cryptographic key which this storage transmitted from the storage is using, It judges whether the cryptographic key which compares the encryption data created by the cryptographic key which read-out / write-in machine is using, and the storage, and read-out / write-in machine are using is in agreement. Said encryption data transmitted from the storage when not in agreement, Judge whether the cryptographic key which compares the encryption data created by the cryptographic key used in the past with read-out / write-in machine, and the storage is using is a cryptographic key used in the past, and a storage is received when it is the cryptographic key used in the past. Transmitting the updating command which makes the cryptographic key which this storage is using update, a storage answers said updating command and updates a cryptographic key.

[0017] The station service system of this invention of claim 8 uses a storage according to claim 1 or 2 as an entrainment card. This entrainment card, It has the automatic ticket gate equipped with read-out / write-in machine according to claim 3 or 4 which performs read-out/writing to this. Read-out / write-in machine The encryption data based on the cryptographic key which this entrainment card transmitted from the entrainment card is using, It judges whether the cryptographic key which compares the encryption data created by the cryptographic key which read-out / write-in machine is using, and the entrainment card, and read-out / write-in machine are using is in agreement. Said encryption data transmitted from the entrainment card when not in agreement, The cryptographic key which compares the encryption data

created by the cryptographic key used in the past with read-out / write-in machine, and the entrainment card is using It judges whether it is the cryptographic key used in the past, and the updating command which makes the cryptographic key which this entrainment card is using update to an entrainment card when it is the cryptographic key used in the past is transmitted, and an entrainment card answers said updating command and updates a cryptographic key.
[0018] The station service system of this invention of claim 9 uses a storage according to claim 1 or 2 as an entrainment card, it has this entrainment card and the card issue machine equipped with read-out / write-in machine according to claim 5 which performs read-out/writing to this, and read-out / write-in machine rewrites two or more cryptographic keys memorized by this entrainment card at the time of issue of an entrainment card.
[0019] The card issue machine of this invention of claim 10 uses a storage according to claim 1 or 2 as an entrainment card, while it writes two or more cryptographic keys which are due to be used the cryptographic key which carries out current use, and in the future in the cryptographic key storage means of this entrainment card, is set as it so that said cryptographic key which carries out current use may be chosen with a cryptographic key selection means, and publishes this entrainment card for it.
[0020] (Operation) Since cipher processing is performed in cipher processing between read-out / write-in machine using either of two or more cryptographic keys according to the storage of claim 1 Since the cryptographic key which the security nature of the whole system is not spoiled and is used is also updated if needed by the command from read-out / write-in machine even if one common cryptographic key is decoded like a common cryptographic key method A possibility that all cryptographic keys may be monitored and decoded is low like the conventional example using all cryptographic keys at random.
[0021] According to the storage of claim 2, by the time two or more cryptographic keys memorized will be altogether used by updating, some [at least] cryptographic keys of two or more cryptographic keys can be rewritten from read-out / write-in machine to a new cryptographic key. By this, updating to a new cryptographic key is attained permanently.
[0022] Since the cryptographic key which judges whether the cryptographic key which the storage is using is a cryptographic key used in the past with read-out / write-in machine according to read-out / the write-in machine of claim 3, sends out an updating command to a storage when it is the cryptographic key used in the past, and a storage uses can be updated, the cryptographic key of a storage can be made in agreement with the newest cryptographic key which read-out / write-in machine is using now.
[0023] Since the cryptographic key used with the command from a high order device is changed according to read-out / the write-in machine of claim 4 The need is accepted. At for example, when [periodical or when there is a possibility that the cryptographic key which is carrying out current use may be decoded] The cryptographic key used with the command from a high order device can be changed into a new cryptographic key, and the cryptographic key which a storage uses according to an operation of claim 3 can also make it further in agreement with the changed cryptographic key.
[0024] Since some [at least] cryptographic keys of two or more cryptographic keys which the storage has memorized are rewritten according to read-out / the write-in machine of claim 5, by the time all the cryptographic keys with which renewal of sequential is carried out and the cryptographic keys of a storage are remembered to be will be used, it can rewrite to a new cryptographic key, and updating to a new cryptographic key is permanently attained by this.
[0025] If the cryptographic key of a card is a cryptographic key used in the past even if the cryptographic key of a card, and a read-out / write-in machine is not in agreement according to the card system of claim 6, since the cryptographic key of a card is updated and it is in agreement with the cryptographic key of read-out / write-in machine, mutual recognition becomes possible.
[0026] According to the cryptographic key operation of claim 7, read-out / write-in machine By comparing the encryption data from a storage with the created encryption data Judge whether the cryptographic key of a storage is in agreement with the cryptographic key which read-out / write-in machine is using, and when not in agreement Since it judges whether the cryptographic key of a storage is a cryptographic key used in the past with read-out / write-in machine, and the cryptographic key of a storage is made to update when it is the past cryptographic key, the cryptographic key of the cryptographic key of a storage, and a read-out / write-in machine can be made in agreement.
[0027] According to the station service system of claim 8, it sets to cipher processing between an entrainment card, and read-out / write-in machine of an automatic ticket gate. An entrainment card, and

read-out / write-in machine Even if a common cryptographic key is decoded like [since two or more cryptographic keys are memorized] the common cryptographic key method which has memorized only one common cryptographic key, the security nature of the whole system is not spoiled. Moreover, since the cryptographic key to be used is also updated if needed by the command from read-out / write-in machine, a possibility that all cryptographic keys may be monitored and decoded is low like the conventional example using all cryptographic keys at random.

[0028] According to the station service system of claim 9, since a card issue machine rewrites two or more cryptographic keys memorized by the entrainment card at the time of issue of an entrainment card, updating of it to a new cryptographic key is attained permanently.

[0029] While writing in two or more cryptographic keys which are due to be used the cryptographic key which carries out current use, and in the future, without according to the card issue machine of claim 10 performing mutual recognition etc. at the time of issue of the completely new entrainment card which is not used rather than collecting the entrainment cards used till then and publishing as a new entrainment card, it sets up and an entrainment card can be published so that the cryptographic key which carries out current use may be chosen.

[0030]

[Embodiment of the Invention] Hereafter, a drawing explains the gestalt of operation of this invention to a detail.

[0031] Drawing 1 is drawing showing the whole station service system configuration to which this invention is applied, and is set to this drawing. 7 Entrainment cards, such as a commuter pass as a storage (for example, non-contact communication link IC card), Read-out / write-in machine with which 6 performs a non-contact communication link between this entrainment card 7 (reader/writer), The automatic ticket gate with which 1 was equipped with read-out / write-in machine 6, the card issue machine with which 4 was equipped with read-out / write-in machine 6, and 5 are the settlement-of-accounts machines equipped with read-out / write-in machine 6, and 25 is a host computer which controls these. An automatic ticket gate 1 and two or more settlement-of-accounts machines 4 are installed within the enclosure of a station.

[0032] The entrainment card 7 is published with the card issue machine 4. Data, such as the entrainment section and a use expiration date, are recorded on this published entrainment card 7. A user receives the ticket gate of an automatic ticket gate 1 using published entrainment card **. The card issue machine 4 and the automatic ticket gate 1 are equipped with read-out / write-in machine 6. The card issue machine 4 and an automatic ticket gate 1 serve as a high order device to read-out / write-in machine 6. Moreover, a host computer 25 serves as a high order device to the card issue machine 4, an automatic ticket gate 1, etc. The automatic ticket gate 1 is equipped with that of CPU26, a host computer 25, and the read-out / write-in machine 6, the interface circuitries 27 and 28 of a between, memory 29, the door control circuit 30, etc., and the card issue machine 4 is equipped with the control panel 35 for the interface circuitries 32 and 33 between CPU31, a host computer 25, and read-out / write-in machine 6, memory 34, and card issue etc. In addition, the reference mark used by the below-mentioned explanation is given to the block which constitutes read-out / write-in machine 6.

[0033] Here, in advance of explanation of the main configurations of a system, the outline about the operation of the cryptographic key of the gestalt of this operation is explained.

[0034] Between the entrainment card 7, and read-out / write-in machine 6, in order to secure security nature, the authentication and the communication link which used the cryptographic key are performed, but in order to cancel the fault of code mode of processing of the conventional example, it constitutes from a gestalt of this operation as follows.

[0035] Namely, two or more cryptographic keys which are due to be used for the entrainment card 7 from now on at the time of card issue are made to memorize. It sets up so that the cryptographic key (for example, cryptographic key which should be used at the card issue time) beforehand defined of two or more of the cryptographic keys may be used. When there is an updating command from read-out / write-in machine 6, it constitutes so that it may update to the cryptographic key specified by the command and the updated cryptographic key may be used.

[0036] Since a large number are published by the target one by one for a long period, the entrainment card 7 The contents of two or more cryptographic keys memorized by the entrainment card 7 are also switched to a new cryptographic key by the target one by one if needed. Therefore, two or more cryptographic keys

memorized by the entrainment card 7 published at the beginning (for example, K1, K2, K3, K4.K5), with two or more cryptographic keys (for example, K2, K3, K4, K5, K6) memorized by the entrainment card 7 published behind, a common cryptographic key (K2, K3, K4, K5) exists, also although kicked While the old cryptographic key (K1) which is not memorized by the next entrainment card 7 is memorized by the original entrainment card 7, on it, the case where the new cryptographic key (K6) which is due to be used in the future which will not be memorized by the original entrainment card 7 is memorized will arise at the next entrainment card 7.

[0037] And two or more cryptographic keys memorized common to all the entrainment cards 7 turn into an usable cryptographic key, and two or more of the cryptographic keys will be used in sequence.

[0038] On the other hand, it was used in the past, and the old cryptographic key (for example, K1) which is not used and the cryptographic key (for example, K2) by which current use is carried out are memorized at least by read-out / write-in machine 6, and current uses this cryptographic key (for example, K2) for it.

[0039] Furthermore, in read-out / write-in machine 6, it sets to the communication link between the entrainment cards 7. If it is the cryptographic key (for example, K1) by which the cryptographic key which the entrainment card 7 is using was used in the past, and current use is not carried out from the response of the entrainment card 7 An updating command is sent out so that it may update to the entrainment card 7 to the cryptographic key (for example, K2) by which current use is carried out, this is answered and the entrainment card 7 is updated to the cryptographic key (for example, K2) by which current use is carried out.

[0040] Therefore, the old entrainment card 7 published at the beginning will be updated and unified into the cryptographic key (for example, K2) by which current use is finally carried out by the communication link with read-out / write-in machine 6.

[0041] In order to secure the security nature of a system, periodically or when there is a possibility that the cryptographic key by which current use is carried out might be decoded With the change command from the automatic ticket gate 1 which is a high order device, read-out / write-in machine 6 While changing into a use way cryptographic key (for example, K3) next the cryptographic key (for example, K2) which is carrying out current use, the cryptographic key (K2) which was being used till then is added as an old cryptographic key, and this changed cryptographic key (K3) is used henceforth. Therefore, in this time, two or more cryptographic keys (for example, K1, K2) by which used it for read-out / write-in machine 6 in the past, and current use is not carried out, and the cryptographic key (for example, K3) by which current use is carried out will be memorized.

[0042] By the communication link with read-out / write-in machine 6, and the entrainment card 7 which changed the cryptographic key with the change command from a high order device While the entrainment card 7 is using the cryptographic key (for example, K2) currently used for the past by which current use is not carried out Read-out / write-in machine 6 sends out an updating command so that it may update to the entrainment card 7 to the cryptographic key (for example, K3) by which current use is carried out, answers this and updates the entrainment card 7 to the cryptographic key (for example, K3) by which current use is carried out.

[0043] Therefore, the entrainment card 7 will be updated and unified into the cryptographic key (for example, K3) by which current use is finally carried out by the communication link with read-out / write-in machine 6.

[0044] Thus, since renewal of sequential of two or more cryptographic keys is carried out if needed and cipher processing is performed Since the cryptographic key which the security nature of the whole system is not spoiled and is used is also updated if needed by the updating command from read-out / write-in machine 6 even if one common cryptographic key is decoded like a common cryptographic key method A possibility that all cryptographic keys may be monitored and decoded is low like the conventional example using all cryptographic keys at random.

[0045] Furthermore, since renewal of the cryptographic key of the entrainment card 7 was also performed by the updating command by the communication link with read-out / write-in machine 6, it did not need to be said that two or more cryptographic keys of all the entrainment cards 7 were changed all at once.

[0046] Hereafter, the main configurations of this entrainment card 7, and a read-out / write-in machine 6 grade are explained to a detail.

[0047] Drawing 2 is the appearance perspective view of the automatic ticket gate 1 equipped with read-out / write-in machine of the gestalt of this operation, and this automatic ticket gate 1 separates the

ticket gate path 36, and is equipped with the body 2 of a ticket gate machine of the pair which carries out phase opposite. In each side face of the body 2 of both the ticket gate machine, the door which permits or prevents passage of the ticket gate path 36 and which is not illustrated is arranged. In each body 2 of a ticket gate machine, read-out / write-in machine 6 is formed, and it is arranged so that the antenna coil 23 may attend the top face of each body 2 of a ticket gate machine.

[0048] When the antenna coil with which the entrainment cards 7, such as a commuter pass, are equipped is located in a communications area, data communication is possible for this antenna coil 23 between the antenna coil of that entrainment card 7 non-contact. As shown in drawing 2 , the data communication of the user who carries the entrainment card 7 becomes possible only by [with the antenna coil 23 of read-out / write-in machine 6 in which the entrainment card 7 was formed by the body 2 of a ticket gate machine] holding up to the communications area for a communication link.

[0049] Read-out / write-in machine 6 communicates with the entrainment card 7, and the automatic ticket gate 1 which is a high order device judges truth, entrainment conditions, etc. of the entrainment card 7 based on the communication link, and controls, opens wide or stops a door based on this.

[0050] The entrainment card 7 of the gestalt of this operation has memorized two or more cryptographic keys as mentioned above. Encryption and a decryption are performed using one certain cryptographic key out of the cryptographic key of these plurality. Moreover, two or more cryptographic keys of all that updated to the cryptographic key which uses for a degree the cryptographic key which is carrying out current use with the updating command of read-out / write-in machine 6 of an automatic ticket gate 1, and have been memorized at the time of card issue with read-out / write-in machines, such as the card issue machine 4, are made to be rewritten. In addition, it is not two or more cryptographic keys of all of the entrainment card 7, and you may make it rewrite only a used cryptographic key to a new cryptographic key at the time of card issue.

[0051] Hereafter, the entrainment card 7 is explained with reference to drawing 3 . The entrainment card 7 has CPU8, program memory 9, data memory 10, the cryptographic key storage memory 11, the code circuit 12, the strange recovery power circuit 13, and antenna coil 14 inside.

[0052] CPU8 processes data transmission to read-out / write-in machine 6 while performing processing based on the command from read-out / write-in machine 6 received through antenna coil 14 using the program data stored in program memory 9, and the working data stored in data memory 10.

[0053] It writes in the command sent out to the entrainment card 7 from card read-out / write-in machine 6 with polling, authentication, and read-out of data, and it has prohibition etc. CPU8 receives such a sending-out command from card read-out / write-in machine 6 with antenna coil 14, and restores to it in the strange demodulator circuit 13, and while incorporating and analyzing after making it process to decode in the code circuit 12 etc., processing according to this analyzed command is performed.

[0054] Two or more cryptographic keys (a cryptographic key 1, a cryptographic key 2, a cryptographic key 3, --, a cryptographic key n) the entrainment card 7 is due to use between read-out / write-in machine 6 of an automatic ticket gate 1 from now on are made to memorize as a cryptographic key storage means, with read-out / write-in machine 6 of the card issue machine 4 at the time of issue of the entrainment card 7, as drawing 4 shows by the cryptographic key storage memory 11. It can read a cryptographic key no longer from the exterior unjustly, read-out of the cryptographic key of these [from the cryptographic key storage memory 11] plurality being used as the hardware configuration which is impossible at all from the outside. What is necessary is for this hardware configuration to form the cryptographic key storage memory 11 in the same LSI chip as CPU8, not to output a cryptographic key, even if it applies a test pin to this LSI chip and gives a signal, or to lose a test terminal, and only for CPU8 in an LSI chip to be able to be made to perform read-out of the data from the cryptographic key storage memory 11, and just to make it not take out the bus between CPU8 and the cryptographic key storage memory 11 as a terminal out of an LSI chip. Read-out of a cryptographic key can be prevented from the ability doing entirely from the exterior of an LSI chip by this (outside a circuit).

[0055] CPU8 chooses the cryptographic key 1 of drawing 4 memorized by the cryptographic key storage memory 11, a cryptographic key 2, a cryptographic key 3, --, one cryptographic key beforehand set up from the cryptographic key n as a cryptographic key selection means, and inputs this into the code circuit 12. Usually, at the time of card issue, since the cryptographic key 1 currently used at the time, two or more cryptographic keys 2 and 3 of the schedule used in order from now on, and -- are made to memorize, it is set up at the beginning as a cryptographic key which should use a cryptographic key 1.

[0056] Then, if there is an updating command from read-out / write-in machine 6 of an automatic ticket gate 1, CPU8 will input this into the code circuit 12, after updating a setup to other cryptographic keys specified by the updating command from the cryptographic key by which a current setup is carried out as a renewal means of a cryptographic key according to the command.
[0057] The code circuit 12 decrypts by enciphering using the cryptographic key chosen as mentioned above, and is used also in mutual recognition with read-out / write-in machine 6 of an automatic ticket gate 1. Of course, the entrainment card 7 in the gestalt of this operation receives read-out of data and the command of writing only after the mutual recognition between read-out / write-in machine 6.
[0058] The strange recovery power circuit 13 generates the power source of the entrainment card 7 by the transmitting field from read-out / write-in machine 6 which won popularity with the modulation of the data transmitted to read-out / write-in machine 6 of an automatic ticket gate 1, the recovery of data which received from read-out / write-in machine 6, and antenna coil 14.
[0059] A cryptographic key storage means for read-out / write-in machine 6 of the gestalt of this operation to be constituted so that authentication and a communication link may be performed between the entrainment cards 7 using a cryptographic key, and to memorize two or more cryptographic keys, A cryptographic key selection means to choose either from from among two or more cryptographic keys memorized by said cryptographic key storage means, A cryptographic key learning means to get to know whether the cryptographic key current use is carried out [the cryptographic key] with the entrainment card by the response from said entrainment card is a cryptographic key of the gap used in the past, At the time of the cryptographic key for which the cryptographic key by which current use is carried out with the entrainment card was used in the past A command sending-out means to send out the command which updates the cryptographic key of an entrainment card, and a cryptographic key modification means to change the cryptographic key which read-out / the write-in machine concerned use with the command from a high order device are provided.
[0060] Hereafter, with reference to drawing 5 , read-out / write-in machine 6 is explained. This read-out / write-in machine 6 have CPU15, program memory 16, data memory 17, the code circuit 18, the cryptographic key storage memory 19 for entrainment cards, the cryptographic key storage memory 20 for high order devices, the interface 21 for high order devices, the strange demodulator circuit 22, and antenna coil 23. A high order device is an automatic ticket gate 1 or the card issue machine 4 as mentioned above.
[0061] An automatic ticket gate 1 controls the drive of a door other than read-out / write-in machine 6, or communicates with a host computer 25, and is connected through the interface 21 for high order devices of read-out / write-in machine 6.
[0062] Read-out / write-in machine 6 performs mutual recognition to a power up also between the automatic ticket gates 1 which are high order devices, secures the security nature of connection and performs processing according to the application in high order devices, such as an automatic ticket gate after it.
[0063] In order to secure the security nature of a system, the duration of service of the cryptographic key by which current use is carried out reaches at a fixed period, or or when there is a possibility that the cryptographic key by which current use is carried out might be decoded The command which changes the cryptographic key which is carrying out current use from the host computer 25 to CPU15 of read-out / write-in machine 6 through the automatic ticket gate 1 which is a high order device is given. For example, by this The cryptographic key of the cryptographic key storage memory 19 for entrainment cards is rewritten like the after-mentioned, and is changed. Then, read-out / write-in machine 6 performs processing with the entrainment card 7 by the changed cryptographic key.
[0064] Drawing 6 is drawing showing an example of the duration of service of a cryptographic key. This example If it passes favorably, without the situation of decode of a cryptographic key arising, it will be what changes a cryptographic key every three months. A cryptographic key 1 If it is already used for three months from January 1, 1998 to March [of the same year] 31, a cryptographic key 2 is current using it after that and it passes favorably A cryptographic key 2 is due to be used till June 30, 1998, and a cryptographic key 3 is due to be changed into a cryptographic key 3 and to be used from July 1, 1998.
[0065] Next, actuation of read-out / write-in machine 6 is explained. Read-out / write-in machine 6 decodes the command received from high order devices, such as an automatic ticket gate 1, through the interface 21 for high order devices, analyzes the decoded command by CPU15, and performs processing according to the command. If the command from a high order device is a command of reading data called

the shelf-life of the data about the entrainment card 7 memorized by the data memory 10 of the entrainment card 7, for example, a commuter pass, and the entrainment section of a commuter pass After making it encipher in the code circuit 18 using the cryptographic key chosen from the cryptographic key storage memory 19 for entrainment cards and modulating the lead command which reads data in the data memory 10 of the entrainment card 7 in the strange demodulator circuit 22, it transmits to the entrainment card 7 from antenna coil 23. And if the response returned from the entrainment card 7 to said lead command is received, it restores to it in the strange demodulator circuit 22, and after decoding in the code circuit 18, the data of the entrainment card 7 will be obtained. And the data is enciphered in the code circuit 18, and it transmits to a high order device from the interface 21 for high order devices as a response. And from this response, the high order device 1, for example, an automatic ticket gate, will open a closing motion door, if the entrainment card 7 is just, and if not just, it will control it not to open a closing motion door.

[0066] Here, there are the renewal command of a cryptographic key of the entrainment card 7 and the cryptographic key rewriting command of the entrainment card 7 other than the command from the former, such as polling, authentication, read-out of data, and writing, among the commands given to the entrainment card 7 from read-out / write-in machine 6. Moreover, there are the renewal command of a cryptographic key of the entrainment card 7, the cryptographic key rewriting command of the entrainment card 7, and the cryptographic key rewriting command of card read-out / write-in machine 6 other than the command from the former, such as read-out of data to a communication link command with the entrainment card 7, authentication, card read-out / write-in machine 6 and writing, among the commands which are high order devices from an automatic gate machine, a card issue machine, etc.

[0067] The cryptographic key (the old cryptographic key - m, --, the old cryptographic key -1) which was being used in the past between the entrainment cards 7 as drawing 7 showed the cryptographic key storage memory 19 for entrainment cards, and the cryptographic key (the present cryptographic key 0) used now are memorized. The cryptographic key storage memory 19 for entrainment cards is only for writing, serves as a hardware configuration which reads from the exterior and is impossible, and has come to be unable to perform read-out of the inaccurate cryptographic key from the outside. Since it mentioned above about this hardware configuration, that explanation is omitted. The encryption for entrainment card 7 processing and decode are performed using the cryptographic key by which current use is carried out among two or more cryptographic keys memorized by this cryptographic key storage memory 19 for entrainment cards.

[0068] Moreover, if the command which should change the cryptographic key which is carrying out current use from the automatic ticket gate 1 which is a high order device is given According to the change command, the present cryptographic key 0 of drawing 7 is rewritten by the cryptographic key which should be changed. The present cryptographic key 0 currently used till then turns into the old cryptographic key -1, the old cryptographic key -1 till then turns into the old cryptographic key -2, and is hereafter rewritten by the contents passed around, and processing is performed henceforth using this rewritten present cryptographic key 0. In addition, what is necessary is to overwrite and just to eliminate the oldest cryptographic key, since it becomes unnecessary when a possibility that it may be used with all the entrainment cards 7 published is lost.

[0069] Moreover, although it was made to be rewritten by the change command from a high order device, as a gestalt of other operations of this invention, the cryptographic key which read-out / write-in machine 6 uses may make two or more cryptographic keys to be used also in read-out / write-in machine 6 from now on memorize beforehand, and it may consist of gestalten of this operation so that the cryptographic key which carries out current use with the updating command from a high order device may be changed.

[0070] The code circuit 18 performs encryption of a plaintext, and decode of a cipher using a cryptographic key, and is used also in the mutual recognition of a high order device besides encryption of correspondence (a command, response) with a high order device or the entrainment card 7, and decode, and the entrainment card 7. The entrainment card 7 usually receives other commands after termination of mutual recognition with read-out / write-in machine 6.

[0071] Next, the processing in an automatic ticket gate 1 is explained with reference to the flow chart shown by drawing 8 .

[0072] When there is no entrainment card 7 into the communications area which can communicate with read-out / write-in machine 6 of the body 2 of a ticket gate machine, as for read-out / write-in machine 6,

the polling command is always sent out from antenna coil 23 the fixed period of 10 ms extent (step n1). If the entrainment card 7 advances into said communications area and the response to a polling command is returned from the entrainment card 7 (step n2), mutual recognition between read-out / write-in machine 6, and the entrainment card 7 will be performed (step n3). This mutual recognition is explained later using drawing 9 . If mutual recognition is O.K., the writing of read-out of the data of the entrainment card 7 and the data to the entrainment card 7 will be processed (step n4), and prohibition of a response will be processed so that the entrainment card [finishing / processing] 7 may not answer the last to polling of as opposed to the following entrainment card 7 in read-out / write-in machine 6 (step n5).

[0073] Next, said mutual recognition is explained with reference to drawing 9 .

[0074] The random data Dr are sent out from read-out / write-in machine 6 to the entrainment card 7 (step n10). The entrainment card 7 enciphers the random data D using the cryptographic key currently used with this entrainment card 7, makes it encryption data Dr', and transmits the enciphered data Dr' to read-out / write-in machine 6. It enciphers using cryptographic key K (0) which receives the data Dr' and which is, on the other hand (step n11), carrying out current use of the random data Dr, and read-out / write-in machine 6 obtains encryption data Dr' (0) (step n12). And although the entrainment card 7 will attest with the right entrainment card 7 if both data Dr' (0) and Dr' of write-in machine [read-out /] 6 correspond as compared with encryption data Dr' to which the enciphered data Dr' (0) has been transmitted from the entrainment card 7 (step n13) When not in agreement, it becomes whether the entrainment card 7 is the inaccurate entrainment card 7 or the cryptographic key which the entrainment card 7 is using is an old cryptographic key.

[0075] When the entrainment card 7 attests with a right entrainment card, shortly, the random data Dc are received from the entrainment card 7 (step n21), this random data Dc is enciphered by cryptographic key K (0) which is carrying out current use (step n22), and it sends out to the entrainment card 7 as encryption data Dc' (step n23). If the response to this sending out is received from the entrainment card 7 (step n24), in Authentication O.K., (step n25) and mutual recognition are completed from receiving contents (step n26), and when it is not O.K., it will consider as mutual recognition NG (step n27).

[0076] In step n13, when the entrainment card 7 does not attest with a right entrainment card After initializing the number of a cryptographic key to 0 (n= 0), read-out / write-in machine 6 (Step n14), It is made the number of the old cryptographic key which was using the number of a cryptographic key in the past (n=n +1) (step n15), data are enciphered using cryptographic key [of this number] K (n) (step n17), and it judges whether it is in agreement with the cipher returned from the entrainment card 7 (step n18). Sequential selection of the old cryptographic key which card read-out / write-in machine 6 has memorized is made until it can judge it as coincidence (step n16). In the case where the number became Dr'=Dr' (n) by the old cryptographic key of n, and it is in agreement, card read-out / write-in machine 6 So that the cryptographic key which the entrainment card 7 was using may judge it as cryptographic key K with the old number (n) and it may update to the entrainment card 7 to cryptographic key K (0) by which current use is carried out Namely, the entrainment card 7 which is using the cryptographic key of the pointer n of the cryptographic key storage memory 11 is received. The renewal command of a cryptographic key is sent out so that it may update to the cryptographic key of a pointer 0 (step n19), and K (0) is made to update the cryptographic key which the entrainment card 7 uses, processing after step n21 is performed, and it attests with the entrainment card 7 being just.

[0077] Moreover, it may be made to attest again after renewal of the cryptographic key of the entrainment card 7 using a new cryptographic key. In addition, when the cipher of the cryptographic keys [neither of] of the old cryptographic key which read-out / write-in machine 6 holds corresponds, the entrainment card 7 is judged to be the inaccurate entrainment card 7 (step n20).

[0078] Next, processing by read-out / write-in machine 6 of the card issue machine 4 is explained.

[0079] It is the same as that of drawing 8 about polling, response reception, and mutual recognition O.K. as shown by drawing 10 in the card issue machine 4. After mutual recognition is completed by drawing 10 , a cryptographic key rewriting command is transmitted and rewriting of the data containing the cryptographic key of the entrainment card 7 is processed (step n4). Two or more cryptographic keys of the cryptographic key storage memory 11 of the entrainment card 7 are rewritten to the cryptographic key which carries out current use, and two or more cryptographic keys which are due to be used from now on in that case (step n5). By this, the cryptographic key which carries out current use is chosen and used for the entrainment card 7 at the beginning, and the cryptographic key used with an updating command is updated henceforth

in order.
[0080] In addition, what is necessary is just to write in the cryptographic key which carries out current use, and two or more cryptographic keys which are due to be used from now on, without performing mutual recognition, when an entrainment card collects the used card, and does not publish them but it completely publishes an entrainment card newly.
[0081] With the gestalt of above-mentioned operation, also although it applies and excels in station service systems, such as an automatic wicket, this invention is not limited to this system and applied also to an automatic toll collection system or its alien system.
[0082] Moreover, with the gestalt of above-mentioned operation, also although it applies and excels in the communication link of a non-contact method, this invention may be applied also to the communication link of a contact method.
[0083]
[Effect of the Invention] According to this invention, the following effectiveness can be acquired as mentioned above.
[0084] Since cipher processing is performed in cipher processing between read-out / write-in machine using either of two or more cryptographic keys according to the storage of this invention of claim 1 Since the cryptographic key which the security nature of the whole system is not spoiled and is used is also updated if needed by the command from read-out / write-in machine even if one common cryptographic key is decoded like a common cryptographic key method At random, like the conventional example using all cryptographic keys, a possibility that all cryptographic keys may be monitored and decoded is low, and security nature improves.
[0085] According to the storage of this invention of claim 2, since some [at least] cryptographic keys of two or more cryptographic keys can be rewritten from read-out / write-in machine, by the time two or more cryptographic keys memorized will be altogether used by updating, it can rewrite to a new cryptographic key, and by this, updating to a new cryptographic key is attained permanently, and security nature can be secured permanently.
[0086] According to read-out / the write-in machine of this invention of claim 3, the cryptographic key which the storage is using When it is the cryptographic key which judges whether it is the cryptographic key used in the past, and was used in the past with read-out / write-in machine Since the cryptographic key which sends out an updating command to a storage and a storage uses for it can be updated, the cryptographic key of a storage can be made in agreement with the newest cryptographic key which read-out / write-in machine is using now. Therefore, in order to change the cryptographic key which a storage uses, it is not necessary to collect storages and to do the difficult activity of changing cryptographic keys all at once, and a cryptographic key will be automatically changed by using a storage and communicating between read-out / write-in machine.
[0087] Since the cryptographic key used with the command from a high order device is changed according to read-out / the write-in machine of this invention of claim 4 The need is accepted. At for example, when [periodical or when there is a possibility that the cryptographic key which is carrying out current use may be decoded] The cryptographic key used with the command from a high order device can be changed into a new cryptographic key, security nature can be secured, and the cryptographic key which a storage uses according to an operation of claim 3 can also be made further in agreement with the changed cryptographic key.
[0088] Since some [at least] cryptographic keys of two or more cryptographic keys which the storage has memorized are rewritten according to read-out / the write-in machine of this invention of claim 5, by the time all the cryptographic keys with which renewal of sequential is carried out and the cryptographic keys of a storage are remembered to be will be used, it can rewrite to two or more new cryptographic keys, and by this, updating to a new cryptographic key is attained permanently, and security nature can be secured permanently.
[0089] If the cryptographic key of a card is a cryptographic key used in the past with read-out / write-in machine even if the cryptographic key of a card, and a read-out / write-in machine is not in agreement according to the card system of this invention of claim 6, since the cryptographic key of a card is updated and it is in agreement with the cryptographic key of read-out / write-in machine, mutual recognition becomes possible. And since the storage is used as the card, it can carry out suitable for various kinds of applications, such as an automatic tariff collecting system, and claim 1 thru/or the operation effectiveness

of 5 can be notably done so.
[0090] According to the cryptographic key operation of this invention of claim 7, read-out / write-in machine By comparing the encryption data from a storage with the created encryption data Judge whether the cryptographic key of a storage is in agreement with the cryptographic key which read-out / write-in machine is using, and when not in agreement Since it judges whether the cryptographic key of a storage is a cryptographic key used in the past, and the cryptographic key of a storage is made to update when it is the past cryptographic key, the cryptographic key of the cryptographic key of a storage, and a read-out / write-in machine can be made in agreement.
[0091] Moreover, since the storage, and read-out / write-in machine have memorized two or more cryptographic keys Even if a common cryptographic key is decoded like the common cryptographic key method which has memorized only one common cryptographic key, the security nature of the whole system is not spoiled. Moreover, since the cryptographic key to be used is also updated if needed by the command from read-out / write-in machine At random, like the conventional example using all cryptographic keys, a possibility that all cryptographic keys may be monitored and decoded was low, and it did not need to be said further that two or more cryptographic keys memorized by the storage were changed all at once.
[0092] According to the station service system of this invention of claim 8, it sets to cipher processing between an entrainment card, and read-out / write-in machine of an automatic ticket gate. An entrainment card, and read-out / write-in machine Even if a common cryptographic key is decoded like [since two or more cryptographic keys are memorized] the common cryptographic key method which has memorized only one common cryptographic key, the security nature of the whole system is not spoiled. Moreover, since the cryptographic key to be used is also updated if needed by the command from read-out / write-in machine At random, like the conventional example using all cryptographic keys, a possibility that all cryptographic keys may be monitored and decoded was low, and it did not need to be said further that two or more cryptographic keys memorized by the entrainment card were changed all at once.
[0093] According to the station service system of this invention of claim 9, at the time of issue of an entrainment card, since two or more cryptographic keys memorized by the entrainment card are rewritten, updating of a card issue machine to a new cryptographic key is attained permanently, and it can secure the security nature of a system permanently.
[0094] While writing in two or more cryptographic keys which are due to be used the cryptographic key which carries out current use, and in the future, without performing mutual recognition etc. not using the collected entrainment card at the time of issue of a completely new entrainment card according to the card issue machine of this invention of claim 10, it sets up so that the cryptographic key which carries out current use may be chosen, and an entrainment card can be published.

[Translation done.]

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1] It is the outline block diagram of the system concerning the operation gestalt of this invention.
[Drawing 2] It is the perspective view of an automatic ticket gate.
[Drawing 3] It is the block diagram of an entrainment card.
[Drawing 4] It is drawing showing the contents of storage of the cryptographic key storage memory of an entrainment card.
[Drawing 5] It is the block diagram of read-out / write-in machine.
[Drawing 6] It is drawing showing the duration of service of a cryptographic key.
[Drawing 7] It is drawing showing the contents of storage of the cryptographic key storage memory for entrainment cards of read-out / write-in machine.
[Drawing 8] It is the flow chart with which explanation of read-out / write-in machine of an automatic ticket gate of operation is presented.
[Drawing 9] It is the flow chart with which explanation of mutual recognition of operation is presented.
[Drawing 10] It is the flow chart with which explanation of read-out / write-in machine of a card issue machine of operation is presented.
[Description of Notations]
1 Automatic Ticket Gate
6 Read-out / Write-in Machine
7 Entrainment Card
8,15 CPU
11 Cryptographic Key Storage Memory
14 23 Antenna coil
19 Cryptographic Key Storage Memory for Entrainment Cards

[Translation done.]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－92040
（P2000－92040A）
(43)公開日　平成12年３月31日(2000.3.31)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｌ　9/10		Ｈ０４Ｌ　9/00	６２１Ａ	２Ｃ００５
Ｂ４２Ｄ　15/10	５２１	Ｂ４２Ｄ　15/10	５２１	５Ｂ０５８
Ｇ０６Ｋ　17/00		Ｇ０６Ｋ　17/00	Ｓ	５Ｊ１０４
Ｇ０７Ｂ　15/00	５１０	Ｇ０７Ｂ　15/00	５１０	
Ｈ０４Ｌ　9/14		Ｈ０４Ｌ　9/00	６４１	

審査請求　有　　請求項の数10　ＯＬ　（全 13 頁）　　最終頁に続く

(21)出願番号　特願平10－258016

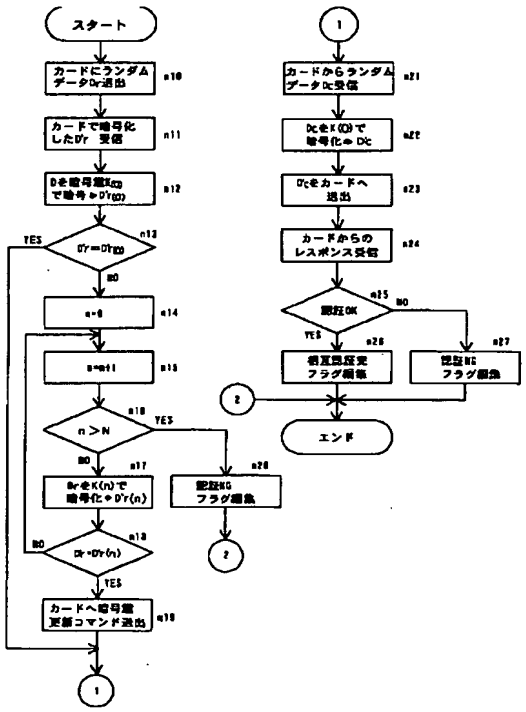
(22)出願日　平成10年９月11日(1998.9.11)

(71)出願人　000002945
オムロン株式会社
京都府京都市右京区花園土堂町10番地
(72)発明者　若林　尚之
京都府京都市右京区花園土堂町10番地　オムロン株式会社内
(74)代理人　100086737
弁理士　岡田　和秀

Ｆターム(参考)　2C005 MA03 MB07 NA09 SA02 SA03
SA05 SA06 SA07 TA21 TA22
5B058 KA11 KA33 KA35 YA20
5J104 AA16 EA02 EA18 NA02 NA33
PA11

(54)【発明の名称】　記憶媒体、読出／書込機、カードシステム、暗号鍵使用方法、駅務システムおよびカード発行機

(57)【要約】
【課題】　ＩＣカードなどの記憶媒体と読出／書込機との間の暗号処理などにおいて、使用する暗号鍵を、必要な時に更新できるとともに、複数の暗号鍵の全てが解読される危険性が低く、記憶媒体に記憶させている複数の暗号鍵を変更することができるようにする。
【解決手段】　ＩＣカードには、ＩＣカード発行時に、そのＩＣカード発行時点で使用している暗号鍵および今後使用する予定の暗号鍵の複数の暗号鍵を記憶させ、読出／書込機には、現在使用している暗号鍵と過去に使用した旧い複数の暗号鍵とを記憶させ、読出／書込機は、ＩＣカードからのリスポンスによって、ＩＣカードが使用している暗号鍵が、過去に使用した暗号鍵であるときには、現在使用している暗号鍵に更新するように更新コマンドを送出し、ＩＣカードは、そのコマンドに応答して使用する暗号鍵を更新するように構成している。



【特許請求の範囲】

【請求項１】　暗号鍵を用いて読出／書込機との間で認証および通信を行うよう構成された記憶媒体において、複数の暗号鍵を記憶する暗号鍵記憶手段と、前記暗号鍵記憶手段に記憶されている複数の暗号鍵のうちからいずれかを選択する暗号鍵選択手段と、前記読出／書込機から送出されるコマンドにより前記選択する暗号鍵を更新する暗号鍵更新手段とを具備したことを特徴とする記憶媒体。

【請求項２】　請求項１において、
前記暗号鍵記憶手段に記憶されている複数の暗号鍵の少なくとも一部の暗号鍵を読出／書込機から書き換えることを特徴とする記憶媒体。

【請求項３】　暗号鍵を用いて記憶媒体との間で認証および通信を行うよう構成された読出／書込機において、複数の暗号鍵を記憶する暗号鍵記憶手段と、前記暗号鍵記憶手段に記憶されている複数の暗号鍵のうちからいずれかを選択する暗号鍵選択手段と、前記記憶媒体からのレスポンスにより該記憶媒体が現在使用している暗号鍵が、当該読出／書込機で過去に使用された暗号鍵であるかどうかを知る暗号鍵知得手段と、前記記憶媒体が現在使用している暗号鍵が過去に使用された暗号鍵のときは、前記記憶媒体の暗号鍵を更新するコマンドを送出する暗号鍵更新コマンド送出手段とを具備したことを特徴とする読出／書込機。

【請求項４】　請求項３において、
上位機器からのコマンドにより、当該読出／書込機が使用する暗号鍵を変更する暗号鍵変更手段を具備したことを特徴とする読出／書込機。

【請求項５】　請求項３において、
前記記憶媒体が記憶している複数の暗号鍵の少なくとも一部の暗号鍵を書き換えることを特徴とする読出／書込機。

【請求項６】　請求項１または２に記載の記憶媒体をカードとし、該カードと、請求項３ないし５いずれかに記載の読出／書込機とを有し、カードが現在使用している暗号鍵が、前記読出／書込機で過去に使用された暗号鍵のときは、カードの暗号鍵を更新した後、その更新された暗号鍵を用いてカードと読出／書込機とが相互認証を行うことを特徴とするカードシステム。

【請求項７】　記憶媒体と読出／書込機それぞれには複数の暗号鍵を記憶させておき、
読出／書込機は、
記憶媒体から送信されてきた該記憶媒体が使用している暗号鍵による暗号化データと、読出／書込機が使用している暗号鍵により作成した暗号化データとを比較して記憶媒体および読出／書込機が使用している暗号鍵が一致しているか否かを判断し、一致していないときには、記憶媒体から送信されてきた前記暗号化データと、読出／書込機で過去に使用した暗号鍵により作成した暗号化データとを比較して記憶媒体が現在使用している暗号鍵が、過去に使用した暗号鍵であるか否かを判断し、前記過去に使用した暗号鍵であるときには、記憶媒体に対して、該記憶媒体が使用している暗号鍵を更新させる更新コマンドを送信し、
記憶媒体は、
前記更新コマンドに応答して、暗号鍵を更新することを特徴とする暗号鍵使用方法。

【請求項８】　請求項１または２に記載の記憶媒体を乗車カードとし、該乗車カードと、これに対する読み出し／書き込みを行う請求項３または４に記載の読出／書込機を備えた自動改札機とを有し、
読出／書込機は、
乗車カードから送信されてきた該乗車カードが使用している暗号鍵による暗号化データと、読出／書込機が使用している暗号鍵により作成した暗号化データとを比較して乗車カードおよび読出／書込機が使用している暗号鍵が一致しているか否かを判断し、一致していないときには、乗車カードから送信されてきた前記暗号化データと、読出／書込機で過去に使用した暗号鍵により作成した暗号化データとを比較して乗車カードが使用している暗号鍵が、過去に使用した暗号鍵であるか否かを判断し、過去に使用した暗号鍵であるときには、乗車カードに対して、該乗車カードが使用している暗号鍵を更新させる更新コマンドを送信し、
乗車カードは、
前記更新コマンドに応答して、暗号鍵を更新することを特徴とする駅務システム。

【請求項９】　請求項１または２に記載の記憶媒体を乗車カードとし、該乗車カードと、これに対する読み出し／書き込みを行う請求項５に記載の読出／書込機を備えたカード発行機とを有し、
読出／書込機は、乗車カードの発行時に、該乗車カードに記憶されている複数の暗号鍵を書き換えることを特徴とする駅務システム。

【請求項１０】　請求項１または２に記載の記憶媒体を乗車カードとし、該乗車カードの暗号鍵記憶手段に、現在使用する暗号鍵および将来使用する予定の複数の暗号鍵を書き込む一方、暗号鍵選択手段で前記現在使用する暗号鍵を選択するように設定して該乗車カードを発行するカード発行機。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、データを記憶する記憶媒体、この記憶媒体に対して読み出し／書き込みを行う読出／書込機、それらを用いたカードシステム、それらに好適な暗号鍵使用方法、および、それらを用いた自動改札などの駅務システム並びにカード発行機に関する。

【０００２】

【従来の技術】例えば、記憶媒体であるカードを自動料金徴収機の読出／書込機でカードの入出金などの処理をする場合、カードのセキュリティ性を確保する必要がある。そのため、通常、カードと読出／書込機との間で暗号を用いた相互認証や通信の暗号化が行われている。なお、相互認証とは、カード側からみて、通信相手となる読出／書込機が正当であるか、また読出／書込機側からみて、通信相手であるカードが正当であるかを、相互に認証することであるが、通常、相互に相手が正当な暗号鍵を知っているかどうかで判定する。

【０００３】

【発明が解決しようとする課題】上述の暗号処理においては、すべてのカードおよび読出／書込機も同じ暗号鍵（共通暗号鍵）を使用するようにした方式があるが、この方式では一旦、共通暗号鍵が他人に知られると、システム全体のセキュリティ性が損なわれてしまうという欠点がある。

【０００４】この欠点をなくすために、カードに複数の暗号鍵を記憶させ、また読出／書込機にもカードが有する複数の暗号鍵を記憶させておき、読出／書込機側ではカードとの間の暗号処理において、前記複数の暗号鍵のうちのいずれか１つの暗号鍵をランダムに用いることでセキュリティ性を高められるようにしたシステムがある。

【０００５】こうした場合に問題とされているのは、前記ランダムに暗号鍵を用いているうちに、複数の暗号鍵のすべてが傍受され解読されてしまう危険性があり、特に、カードと読出／書込機とが非接触で通信を行う場合に、その危険性が増大する。そこで、カードが記憶する複数の暗号鍵のすべてを他の複数の暗号鍵に一斉に変更させることが考えられるが、このような暗号鍵の変更は、多数のカードが発行されて使用されるというカードの利用形態から考えて実際上は不可能である。

【０００６】本発明は、上述の技術的課題に鑑みて為されたものであって、ランダムにすべての暗号鍵を使用するのではなく、必要な時、例えば、定期的あるいは暗号鍵が解読されたような虞れがある時に暗号鍵を更新できるようにし、しかも、記憶媒体の複数の暗号鍵の変更を一斉に行う必要がないようにすることを目的とする。

【０００７】

【課題を解決するための手段】本発明では、上述の目的を達成するために、次のように構成している。

【０００８】すなわち、請求項１の本発明の記憶媒体は、暗号鍵を用いて読出／書込機との間で認証および通信を行うよう構成された記憶媒体において、複数の暗号鍵を記憶する暗号鍵記憶手段と、前記暗号鍵記憶手段に記憶されている複数の暗号鍵のうちからいずれかを選択する暗号鍵選択手段と、前記読出／書込機から送出されるコマンドにより前記選択する暗号鍵を更新する暗号鍵更新手段とを具備している。

【０００９】ここで、更新とは、使用している暗号鍵を、複数の暗号鍵の内の別の暗号鍵に切り換えて使用することをいい、更新の度に、複数の暗号鍵の内の一つの暗号鍵が、それまで使用していた暗号鍵に代えて使用されることになる。

【００１０】また、記憶媒体と読出／書込機との間の通信は、有線方式または無線方式のいずれの方式であってもよい。

【００１１】請求項２の本発明の記憶媒体は、請求項１において、前記暗号鍵記憶手段に記憶されている複数の暗号鍵の少なくとも一部の暗号鍵を読出／書込機から書き換えるものである。

【００１２】請求項３の本発明の読出／書込機は、暗号鍵を用いて記憶媒体との間で認証および通信を行うよう構成された読出／書込機において、複数の暗号鍵を記憶する暗号鍵記憶手段と、前記暗号鍵記憶手段に記憶されている複数の暗号鍵のうちからいずれかを選択する暗号鍵選択手段と、前記記憶媒体からのレスポンスにより該記憶媒体が現在使用している暗号鍵が、当該読出／書込機で過去に使用された暗号鍵であるかどうかを知る暗号鍵知得手段と、前記記憶媒体が現在使用している暗号鍵が過去に使用された暗号鍵のときは、前記記憶媒体の暗号鍵を更新するコマンドを送出する暗号鍵更新コマンド送出手段とを具備している。

【００１３】請求項４の本発明の読出／書込機は、請求項３において、上位機器からのコマンドにより、当該読出／書込機が使用する暗号鍵を変更する暗号鍵変更手段を具備している。

【００１４】請求項５の本発明の読出／書込機は、請求項３において、前記記憶媒体が記憶している複数の暗号鍵の少なくとも一部の暗号鍵を書き換えるものである。

【００１５】請求項６の本発明のカードシステムは、請求項１または２に記載の記憶媒体をカードとし、該カードと、請求項３ないし５いずれかに記載の読出／書込機とを有し、カードが現在使用している暗号鍵が、読出／書込機で過去に使用された暗号鍵のときは、カードの暗号鍵を更新した後、その更新された暗号鍵を用いてカードと読出／書込機とが相互認証を行うものである。

【００１６】請求項７の本発明の暗号鍵使用方法は、記憶媒体と読出／書込機それぞれには複数の暗号鍵を記憶させておき、読出／書込機は、記憶媒体から送信されてきた該記憶媒体が使用している暗号鍵による暗号化データと、読出／書込機が使用している暗号鍵により作成した暗号化データとを比較して記憶媒体および読出／書込機が使用している暗号鍵が一致しているか否かを判断し、一致していないときには、記憶媒体から送信されてきた前記暗号化データと、読出／書込機で過去に使用した暗号鍵により作成した暗号化データとを比較して記憶媒体が使用している暗号鍵が、過去に使用した暗号鍵であるか否かを判断し、過去に使用した暗号鍵であるとき

には、記憶媒体に対して、該記憶媒体が使用している暗号鍵を更新させる更新コマンドを送信し、記憶媒体は、前記更新コマンドに応答して、暗号鍵を更新するものである。

【００１７】請求項８の本発明の駅務システムは、請求項１または２に記載の記憶媒体を乗車カードとし、該乗車カードと、これに対する読み出し／書き込みを行う請求項３または４に記載の読出／書込機を備えた自動改札機とを有し、読出／書込機は、乗車カードから送信されてきた該乗車カードが使用している暗号鍵による暗号化データと、読出／書込機が使用している暗号鍵により作成した暗号化データとを比較して乗車カードおよび読出／書込機が使用している暗号鍵が一致しているか否かを判断し、一致していないときには、乗車カードから送信されてきた前記暗号化データと、読出／書込機で過去に使用した暗号鍵により作成した暗号化データとを比較して乗車カードが使用している暗号鍵が、過去に使用した暗号鍵であるか否かを判断し、過去に使用した暗号鍵であるときには、乗車カードに対して、該乗車カードが使用している暗号鍵を更新させる更新コマンドを送信し、乗車カードは、前記更新コマンドに応答して、暗号鍵を更新するものである。

【００１８】請求項９の本発明の駅務システムは、請求項１または２に記載の記憶媒体を乗車カードとし、該乗車カードと、これに対する読み出し／書き込みを行う請求項５に記載の読出／書込機を備えたカード発行機とを有し、読出／書込機は、乗車カードの発行時に、該乗車カードに記憶されている複数の暗号鍵を書き換えるものである。

【００１９】請求項１０の本発明のカード発行機は、請求項１または２に記載の記憶媒体を乗車カードとし、該乗車カードの暗号鍵記憶手段に、現在使用する暗号鍵および将来使用する予定の複数の暗号鍵を書き込む一方、暗号鍵選択手段で前記現在使用する暗号鍵を選択するように設定して該乗車カードを発行するものである。

【００２０】（作用）請求項１の記憶媒体によれば、読出／書込機との間の暗号処理において、複数の暗号鍵のいずれかを用いて暗号処理を行うので、共通暗号鍵方式のように一つの共通暗号鍵が解読されてもシステム全体のセキュリティ性が損なわれることがなく、また、使用する暗号鍵も読出／書込機からのコマンドによって必要に応じて更新されるので、ランダムにすべての暗号鍵を用いる従来例のように、全ての暗号鍵が傍受されて解読される虞れが低い。

【００２１】請求項２の記憶媒体によれば、記憶されている複数の暗号鍵が更新によって全て使用されてしまうまでに、複数の暗号鍵の少なくとも一部の暗号鍵を読出／書込機から新たな暗号鍵に書き換えることができる。これによって、永続的に新しい暗号鍵への更新が可能となる。

【００２２】請求項３の読出／書込機によれば、記憶媒体が使用している暗号鍵が、読出／書込機で過去に使用された暗号鍵であるか否かを判断し、過去に使用されている暗号鍵であるときには、記憶媒体に更新コマンドを送出して記憶媒体が使用する暗号鍵を更新することができるので、記憶媒体の暗号鍵を、読出／書込機が現在使用している最新の暗号鍵に一致させることができる。

【００２３】請求項４の読出／書込機によれば、上位機器からのコマンドによって使用する暗号鍵が変更されるので、必要に応じて、例えば、定期的あるいは現在使用している暗号鍵が解読される虞れがあるような時に、上位機器からのコマンドによって使用する暗号鍵を、新しい暗号鍵に変更できることになり、さらに、請求項３の作用によって、記憶媒体が使用する暗号鍵もその変更された暗号鍵に一致させることができる。

【００２４】請求項５の読出／書込機によれば、記憶媒体が記憶している複数の暗号鍵の少なくとも一部の暗号鍵を書き換えるので、記憶媒体の暗号鍵が順次更新されて記憶されている全ての暗号鍵が使用されてしまうまでに、新たな暗号鍵に書き換えることができ、これによって、永続的に新しい暗号鍵への更新が可能となる。

【００２５】請求項６のカードシステムによれば、カードと読出／書込機との暗号鍵が一致しなくても、カードの暗号鍵が、過去に使用した暗号鍵であれば、カードの暗号鍵が更新されて読出／書込機の暗号鍵に一致するので、相互認証が可能となる。

【００２６】請求項７の暗号鍵使用方法によれば、読出／書込機は、記憶媒体からの暗号化データと作成した暗号化データとを比較することにより、記憶媒体の暗号鍵が、読出／書込機が使用している暗号鍵に一致しているか否かを判断し、一致していないときには、記憶媒体の暗号鍵が、読出／書込機で過去に使用した暗号鍵であるか否かを判断し、過去の暗号鍵であるときには、記憶媒体の暗号鍵を更新させるので、記憶媒体の暗号鍵と読出／書込機との暗号鍵を一致させることができる。

【００２７】請求項８の駅務システムによれば、乗車カードと自動改札機の読出／書込機との間の暗号処理において、乗車カードおよび読出／書込機は、複数の暗号鍵を記憶しているので、一つの共通暗号鍵のみを記憶している共通暗号鍵方式のように共通暗号鍵が解読されてもシステム全体のセキュリティ性が損なわれることがなく、また、使用する暗号鍵も読出／書込機からのコマンドによって必要に応じて更新されるので、ランダムにすべての暗号鍵を用いる従来例のように、すべての暗号鍵が傍受されて解読される虞れが低い。

【００２８】請求項９の駅務システムによれば、カード発行機は、乗車カードの発行時に、乗車カードに記憶されている複数の暗号鍵を書き換えるので、永続的に新しい暗号鍵への更新が可能となる。

【００２９】請求項１０のカード発行機によれば、それ

まで使用された乗車カードを回収して新たな乗車カードとして発行するのではなく、使用されたことのない全く新規な乗車カードの発行時において、相互認証などを行うことなく、現在使用する暗号鍵および将来使用する予定の複数の暗号鍵を書き込むとともに、現在使用する暗号鍵を選択するよう設定して乗車カードを発行できる。

【００３０】

【発明の実施の形態】以下、図面によって本発明の実施の形態について詳細に説明する。

【００３１】図１は、本発明が適用される駅務システムの全体構成を示す図であり、同図において、７は記憶媒体（例えば、非接触通信ＩＣカード）としての定期券などの乗車カード、６はこの乗車カード７との間で非接触通信を行う読出／書込機（リーダ／ライタ）、１は読出／書込機６を備えた自動改札機、４は読出／書込機６を備えたカード発行機、５は読出／書込機６を備えた精算機であり、２５はこれらを制御するホストコンピュータである。自動改札機１および精算機４は、駅の構内に、複数台設置されている。

【００３２】乗車カード７は、カード発行機４で発行される。この発行された乗車カード７には、乗車区間とか使用有効期限等のデータが記録される。利用者は、発行された乗車カードやを用いて自動改札機１の改札を受ける。カード発行機４も自動改札機１も読出／書込機６を備えている。カード発行機４および自動改札機１は、読出／書込機６に対する上位機器となる。また、ホストコンピュータ２５は、カード発行機４および自動改札機１などに対する上位機器となる。自動改札機１は、ＣＰＵ２６、ホストコンピュータ２５および読出／書込機６のと間のインタフェース回路２７，２８、メモリ２９および扉制御回路３０などを備えており、カード発行機４は、ＣＰＵ３１、ホストコンピュータ２５および読出／書込機６との間のインタフェース回路３２，３３、メモリ３４およびカード発行のための操作盤３５などを備えている。なお、読出／書込機６を構成するブロックには、後述の説明で使用する参照符号を付している。

【００３３】ここで、システムの主要な構成の説明に先立って、この実施の形態の暗号鍵の使用方法についての概要を説明する。

【００３４】乗車カード７と読出／書込機６との間では、セキュリティ性を確保するために、暗号鍵を用いた認証や通信を行うのであるが、この実施の形態では、従来例の暗号処理方式の欠点を解消するために、次のように構成している。

【００３５】すなわち、乗車カード７には、カード発行時に、今後使用する予定の複数の暗号鍵を記憶させておき、その複数の暗号鍵の内の予め定めた暗号鍵（例えば、カード発行時点において使用すべき暗号鍵）を使用するように設定しておき、読出／書込機６からの更新コマンドがあったときには、そのコマンドで指定された暗号鍵に更新してその更新された暗号鍵を使用するように構成している。

【００３６】乗車カード７は、多数が長い期間に亘って順次的に発行されるために、乗車カード７に記憶される複数の暗号鍵の内容も必要に応じて新しい暗号鍵に順次的に切り換えられ、したがって、当初に発行された乗車カード７に記憶されている複数の暗号鍵（例えば、Ｋ１，Ｋ２，Ｋ３，Ｋ４．Ｋ５）と、後に発行される乗車カード７に記憶される複数の暗号鍵（例えば、Ｋ２，Ｋ３，Ｋ４，Ｋ５，Ｋ６）とは、共通する暗号鍵（Ｋ２，Ｋ３，Ｋ４，Ｋ５）が存在するけれども、当初の乗車カード７には、後の乗車カード７に記憶されていない旧い暗号鍵（Ｋ１）が記憶されている一方、後の乗車カード７には、当初の乗車カード７に記憶されていない将来使用する予定の新規な暗号鍵（Ｋ６）が記憶される場合が生じることになる。

【００３７】そして、全ての乗車カード７に共通に記憶されている複数の暗号鍵が、使用可能な暗号鍵となり、その複数の暗号鍵が順番で使用されることになる。

【００３８】一方、読出／書込機６には、過去に使用されて現在は使用されていない旧い暗号鍵（例えば、Ｋ１）および現在使用されている暗号鍵（例えば、Ｋ２）が少なくとも記憶されており、この暗号鍵（例えばＫ２）を使用する。

【００３９】さらに、読出／書込機６では、乗車カード７との間の通信において、乗車カード７のレスポンスからその乗車カード７が使用している暗号鍵が、過去に使用されて現在使用されていない暗号鍵（例えばＫ１）であれば、乗車カード７に対して、現在使用されている暗号鍵（例えばＫ２）に更新するように更新コマンドを送出し、これに応答してその乗車カード７は、現在使用されている暗号鍵（例えばＫ２）に更新するのである。

【００４０】したがって、当初発行された旧い乗車カード７は、読出／書込機６との通信によって、最終的に現在使用されている暗号鍵（例えばＫ２）に更新されて統一されることになる。

【００４１】システムのセキュリティ性を確保するために、定期的に、あるいは、現在使用されている暗号鍵が解読された虞れがあるような時には、上位機器である自動改札機１などからの変更コマンドによって、読出／書込機６は、現在使用している暗号鍵（例えば、Ｋ２）を、次に使用すべ暗号鍵（例えば、Ｋ３）に変更する一方、それまで使用していた暗号鍵（Ｋ２）を、旧い暗号鍵として追加し、以後、この変更した暗号鍵（Ｋ３）を使用する。したがって、この時点では、読出／書込機６には、過去に使用して現在使用されていない複数の暗号鍵（例えば、Ｋ１，Ｋ２）および現在使用されている暗号鍵（例えば、Ｋ３）が記憶されることになる。

【００４２】上位機器からの変更コマンドによって暗号鍵を変更した読出／書込機６と乗車カード７との通信に

よって、乗車カード７が、現在使用されていない過去に使用されていた暗号鍵（例えば、Ｋ２）を使用していたときには、読出／書込機６は、その乗車カード７に対して、現在使用されている暗号鍵（例えばＫ３）に更新するように更新コマンドを送出し、これに応答してその乗車カード７は、現在使用されている暗号鍵（例えばＫ３）に更新するのである。

【００４３】したがって、乗車カード７は、読出／書込機６との通信によって、最終的に現在使用されている暗号鍵（例えばＫ３）に更新されて統一されることになる。

【００４４】このように複数の暗号鍵を必要に応じて順次更新して暗号処理を行うので、共通暗号鍵方式のように一つの共通暗号鍵が解読されてもシステム全体のセキュリティ性が損なわれることがなく、また、使用する暗号鍵も読出／書込機６からの更新コマンドによって必要に応じて更新されるので、ランダムに全ての暗号鍵を用いる従来例のように、全ての暗号鍵が傍受されて解読される虞れが低い。

【００４５】さらに、乗車カード７の暗号鍵の更新も、読出／書込機６との通信による更新コマンドによって行われるので、全ての乗車カード７の複数の暗号鍵を一斉に変更するといった必要がない。

【００４６】以下、この乗車カード７および読出／書込機６等の主要な構成について詳細に説明する。

【００４７】図２は、この実施の形態の読出／書込機を備えた自動改札機１の外観斜視図であり、この自動改札機１は、改札通路３６を隔てて相対向する一対の改札機本体２を備える。両改札機本体２の側面それぞれには、改札通路３６の通過を許可あるいは阻止する図示しない扉が配備されている。各改札機本体２には、読出／書込機６が設けられており、そのアンテナコイル２３が各改札機本体２の上面に臨むように配設されている。

【００４８】このアンテナコイル２３は、定期券等の乗車カード７が備えるアンテナコイルが通信エリア内に位置したときに、その乗車カード７のアンテナコイルとの間で非接触でデータ通信が可能となっている。乗車カード７を携帯する利用者は、図２に示すように、その乗車カード７を改札機本体２に設けられた読出／書込機６のアンテナコイル２３との通信のための通信エリアにかざすだけでデータ通信が可能となる。

【００４９】読出／書込機６は乗車カード７と通信を行い、上位機器である自動改札機１は、その通信に基づいて乗車カード７の真偽および乗車条件などを判定し、これに基づいて、扉を制御して開放したり、閉止したりする。

【００５０】本実施の形態の乗車カード７は、上述のように複数の暗号鍵を記憶しており、それら複数の暗号鍵の中からある１つの暗号鍵を用いて暗号化とか復号化を行い、また、自動改札機１の読出／書込機６の更新コマンドにより現在使用している暗号鍵を次に使用する暗号鍵に更新し、またカード発行機４などの読出／書込機によって、カード発行時に、記憶している複数の全ての暗号鍵が書き換えられるようにしている。なお、カード発行時には、乗車カード７の複数の暗号鍵の全てではなく、使用済みの暗号鍵のみを新たな暗号鍵に書き換えるようにしてもよい。

【００５１】以下、図３を参照して、乗車カード７について説明する。乗車カード７は、内部にＣＰＵ８、プログラムメモリ９、データメモリ１０、暗号鍵記憶メモリ１１、暗号回路１２および変復調電源回路１３ならびにアンテナコイル１４を有している。

【００５２】ＣＰＵ８は、プログラムメモリ９に格納されているプログラムデータと、データメモリ１０に格納されているワーキングデータとを用いて、アンテナコイル１４を通じて受信した読出／書込機６からのコマンドに基づく処理を行うとともに、読出／書込機６に対してデータ送信の処理を行う。

【００５３】カード読出／書込機６から乗車カード７に送出されてくるコマンドには、ポーリング、認証、データの読み出しと書き込み、禁止などがある。ＣＰＵ８は、カード読出／書込機６からのこうした送出コマンドをアンテナコイル１４で受信し、変復調回路１３で復調し、暗号回路１２で復号する等の処理を行わせた後に取り込んで解析するとともに、この解析したコマンドに従った処理を実行するようになっている。

【００５４】暗号鍵記憶メモリ１１には、暗号鍵記憶手段として、図４で示すように乗車カード７の発行時に、カード発行機４の読出／書込機６によって、乗車カード７が自動改札機１の読出／書込機６などとの間で今後使用する予定である複数の暗号鍵（暗号鍵１，暗号鍵２，暗号鍵３，…，暗号鍵ｎ）が記憶させられている。暗号鍵記憶メモリ１１からは、これら複数の暗号鍵の読み出しは外部から一切できないハードウェア構成とされて不正に外部から暗号鍵が読み出せないようになっている。このハードウェア構成は、暗号鍵記憶メモリ１１をＣＰＵ８と同じＬＳＩチップに設け、このＬＳＩチップにテストピンを当てて信号を与えても暗号鍵は出力されず、あるいは、テスト端子をなくし、暗号鍵記憶メモリ１１からのデータの読み出しは、ＬＳＩチップ内のＣＰＵ８のみができるようにし、ＣＰＵ８と暗号鍵記憶メモリ１１間のバスは、ＬＳＩチップの外には、端子として出さないようにすればよい。これによって、ＬＳＩチップの外部（回路の外）から暗号鍵の読み出しを一切できないようにすることができる。

【００５５】ＣＰＵ８は、暗号鍵選択手段として、暗号鍵記憶メモリ１１に記憶されている図４の暗号鍵１，暗号鍵２，暗号鍵３，…，暗号鍵ｎから予め設定されている１つの暗号鍵を選択し、これを暗号回路１２に入力するようになっている。通常、カード発行時には、その時

点で使用されている暗号鍵１と、今後順番に使用されていく予定の複数の暗号鍵２，３，…が記憶させられるので、当初は、暗号鍵１を使用すべき暗号鍵として設定されている。

【００５６】その後、自動改札機１の読出／書込機６から更新コマンドがあれば、ＣＰＵ８は、暗号鍵更新手段として、そのコマンドに従って現在設定されている暗号鍵から更新コマンドで指定された他の暗号鍵に設定を更新したうえで、これを暗号回路１２に入力するようになっている。

【００５７】暗号回路１２は、上述のようにして選択された暗号鍵を用いて暗号化、復号化を行うものであり、自動改札機１の読出／書込機６との相互認証においても使用される。勿論、本実施の形態における乗車カード７は読出／書込機６との間での相互認証の後でのみデータの読み出しや書き込みのコマンドを受け付けるようになっている。

【００５８】変復調電源回路１３は、自動改札機１の読出／書込機６へ送信するデータの変調、読出／書込機６から受信したデータの復調、アンテナコイル１４で受けた読出／書込機６からの送信磁界により乗車カード７の電源を生成するようになっている。

【００５９】本実施の形態の読出／書込機６は、暗号鍵を用いて乗車カード７との間で認証および通信を行うよう構成されたものであって、複数の暗号鍵を記憶する暗号鍵記憶手段と、前記暗号鍵記憶手段に記憶されている複数の暗号鍵のうちからいずれかを選択する暗号鍵選択手段と、前記乗車カードからのレスポンスにより乗車カードで現在使用されている暗号鍵が、過去に使用されたいずれの暗号鍵であるかを知る暗号鍵知得手段と、乗車カードで現在使用されている暗号鍵が過去に使用されていた暗号鍵のときは、乗車カードの暗号鍵を更新するコマンドを送出するコマンド送出手段と、上位機器からのコマンドにより、当該読出／書込機が使用する暗号鍵を変更する暗号鍵変更手段とを具備している。

【００６０】以下、図５を参照して読出／書込機６について説明する。この読出／書込機６は、ＣＰＵ１５、プログラムメモリ１６、データメモリ１７、暗号回路１８、乗車カード用暗号鍵記憶メモリ１９、上位機器用暗号鍵記憶メモリ２０、上位機器用インタフェース２１および変復調回路２２ならびにアンテナコイル２３を有している。上位機器とは、上述のように、自動改札機１あるいはカード発行機４などである。

【００６１】自動改札機１は、読出／書込機６の他に扉の駆動機構を制御したり、ホストコンピュータ２５と通信を行うものであり、読出／書込機６の上位機器用インタフェース２１を介して接続されている。

【００６２】読出／書込機６は、電源投入時に、上位機器である自動改札機１などとの間でも相互認証を行い、接続のセキュリティ性を確保し、それ以降の自動改札機などの上位機器におけるアプリケーションに応じた処理を行うようになっている。

【００６３】システムのセキュリティ性を確保するために、現在使用されている暗号鍵の使用期間が一定期間に達したり、あるいは、現在使用されている暗号鍵が解読された虞れがあるような場合には、例えば、ホストコンピュータ２５から上位機器である自動改札機１などを介して読出／書込機６のＣＰＵ１５に対して、現在使用している暗号鍵を変更するコマンドが与えられ、これによって、乗車カード用暗号鍵記憶メモリ１９の暗号鍵が後述のように書き換えられて変更される。その後、読出／書込機６は、変更した暗号鍵で乗車カード７との処理を行うようになっている。

【００６４】図６は、暗号鍵の使用期間の一例を示す図であり、この例は、暗号鍵の解読といった事態が生じることなく順調に経過すれば、三カ月毎に暗号鍵を変更するものであり、暗号鍵１は、１９９８年１月１日から同年３月３１日までの三カ月間既に使用され、その後、暗号鍵２が現在使用中であり、順調に経過すれば、１９９８年６月３０日まで暗号鍵２が使用される予定であり、１９９８年７月１日からは暗号鍵３に変更されて暗号鍵３が使用される予定である。

【００６５】次に、読出／書込機６の動作について説明する。読出／書込機６は、上位機器用インタフェース２１を通して自動改札機１などの上位機器から受信したコマンドを復号し、復号したコマンドをＣＰＵ１５で解析し、そのコマンドに従った処理を実行する。上位機器からのコマンドが、例えば乗車カード７のデータメモリ１０に記憶されている乗車カード７に関するデータ、例えば定期券の有効期間、定期券の乗車区間というデータを読み出すというコマンドであれば、乗車カード７のデータメモリ１０からデータを読み取るリードコマンドを、乗車カード用暗号鍵記憶メモリ１９から選択した暗号鍵を用いて暗号回路１８で暗号化させ、変復調回路２２で変調させたうえでアンテナコイル２３から乗車カード７に送信する。そして、乗車カード７から前記リードコマンドに対して返送されるレスポンスを受信すると、それを変復調回路２２で復調し、暗号回路１８で復号したうえで乗車カード７のデータを得る。そして、そのデータを、暗号回路１８で暗号化してレスポンスとして上位機器用インタフェース２１から上位機器に送信する。そして、上位機器、例えば自動改札機１は、このレスポンスから乗車カード７が正当であれば開閉ドアを開け、正当でなければ開閉ドアを開けないように制御する。

【００６６】ここで、読出／書込機６から乗車カード７に与えられるコマンドにはポーリング、認証、データの読み出しと書き込みなどの従来からのコマンドの他に、乗車カード７の暗号鍵更新コマンド、乗車カード７の暗号鍵書き換えコマンドがある。また、上位機器である自動改札装置やカード発行機などからのコマンドには、乗

車カード７との通信コマンド、認証、カード読出／書込機６に対するデータの読み出しと書き込みなどの従来からのコマンドの他に、乗車カード７の暗号鍵更新コマンド、乗車カード７の暗号鍵書き換えコマンド、カード読出／書込機６の暗号鍵書き換えコマンドがある。

【００６７】乗車カード用暗号鍵記憶メモリ１９は、図７で示すように乗車カード７との間で過去に使用していた暗号鍵（旧暗号鍵－m，…，旧暗号鍵－１）と現在使用している暗号鍵（現在の暗号鍵０）とが記憶されている。乗車カード用暗号鍵記憶メモリ１９は、書き込み専用であり、外部から読み出しできないハードウェア構成となっていて外部からの不正な暗号鍵の読み出しができないようになっている。このハードウェア構成については前述したのでその説明は省略する。この乗車カード用暗号鍵記憶メモリ１９に記憶されている複数の暗号鍵のうち、現在使用されている暗号鍵を用いて乗車カード７処理のための暗号化、復号が行われる。

【００６８】また、上位機器である自動改札機１などから現在使用している暗号鍵を変更すべきコマンドが与えられると、その変更コマンドに応じて、図７の現暗号鍵０が、変更すべき暗号鍵に書き換えられ、それまで使用されていた現暗号鍵０が、旧暗号鍵－１となり、それまでの旧暗号鍵－１が、旧暗号鍵－２となり、以下、順送りされた内容に書き換えられ、以後は、この書き換えられた現暗号鍵０を使用して処理が行われる。なお、最も旧い暗号鍵は、発行されているすべての乗車カード７で使用される虞れがなくなった時点で不要となるので、上書きして消去すればよい。

【００６９】また、この実施の形態では、読出／書込機６が使用する暗号鍵は、上位機器からの変更コマンドによって書き換えられるようにしたけれども、本発明の他の実施の形態として、読出／書込機６においても、今後使用する複数の暗号鍵を予め記憶させておき、上位機器からの更新コマンドによって現在使用する暗号鍵を変更するように構成してもよい。

【００７０】暗号回路１８は、暗号鍵を用いて平文の暗号化、暗号文の復号を行い、また、上位機器とか乗車カード７との通信文（コマンド、レスポンス）の暗号化、復号の他、上位機器と乗車カード７との相互認証においても使用される。乗車カード７は、通常、読出／書込機６との相互認証の終了後にその他のコマンドを受け付けるようになっている。

【００７１】次に、自動改札機１における処理を図８で示されるフローチャートを参照して説明する。

【００７２】乗車カード７が、改札機本体２の読出／書込機６と通信し得る通信エリア内に無いときは、読出／書込機６は常に１０ミリ秒程度の一定周期でポーリングコマンドをアンテナコイル２３から送出している（ステップｎ１）。前記通信エリアに乗車カード７が進入し、その乗車カード７からポーリングコマンドに対するレスポンスが返送されると（ステップｎ２）、読出／書込機６と乗車カード７との間の相互認証を行う（ステップｎ３）。この相互認証については図９を用いて後で説明する。相互認証がＯＫであれば、乗車カード７のデータの読み出しと乗車カード７へのデータの書き込みの処理を行い（ステップｎ４）、最後に読出／書込機６が次の乗車カード７に対するポーリングに対して、処理済みの乗車カード７が応答しないように応答禁止の処理をする（ステップｎ５）。

【００７３】次に図９を参照して前記相互認証について説明する。

【００７４】読出／書込機６から乗車カード７に対しランダムデータＤｒを送出する（ステップｎ１０）。乗車カード７は、該乗車カード７で使用している暗号鍵を用いてそのランダムデータＤを暗号化して暗号化データＤｒ’とし、その暗号化したデータＤｒ’を読出／書込機６に送信する。読出／書込機６は、そのデータＤｒ’を受信する一方（ステップｎ１１）、そのランダムデータＤｒを現在使用している暗号鍵Ｋ（０）を用いて暗号化して暗号化データＤｒ’（０）を得る（ステップｎ１２）。そして、読出／書込機６はその暗号化したデータＤｒ’（０）を乗車カード７から送信されてきた暗号化データＤｒ’と比較し（ステップｎ１３）、両データＤｒ’（０）とＤｒ’とが一致していれば乗車カード７が正しい乗車カード７と認証するが、一致しないときは乗車カード７が不正な乗車カード７であるか、それとも乗車カード７が使用している暗号鍵が旧い暗号鍵であるかのいずれかとなる。

【００７５】乗車カード７が正しい乗車カードと認証した場合、今度は、乗車カード７からランダムデータＤｃを受信し（ステップｎ２１）、このランダムデータＤｃを現在使用している暗号鍵Ｋ（０）で暗号化し（ステップｎ２２）、暗号化データＤｃ’として、乗車カード７に送出する（ステップｎ２３）。乗車カード７からこの送出に対するレスポンスを受信すると（ステップｎ２４）、受信内容から認証ＯＫの場合は（ステップｎ２５）、相互認証が完了し（ステップｎ２６）、ＯＫでない場合は相互認証ＮＧとする（ステップｎ２７）。

【００７６】ステップｎ１３において、乗車カード７が正しい乗車カードと認証しない場合は、読出／書込機６は、暗号鍵の番号を０に初期化（ｎ＝０）した上で（ステップｎ１４）、暗号鍵の番号を過去に使用していた旧い暗号鍵の番号にし（ｎ＝ｎ＋１）（ステップｎ１５）、この番号の暗号鍵Ｋ（ｎ）を用いてデータを暗号化し（ステップｎ１７）、乗車カード７から返送されてきた暗号文と一致するかを判断する（ステップｎ１８）。一致と判断できるまで、カード読出／書込機６が記憶している旧い暗号鍵を順次選択していき（ステップｎ１６）、番号がｎの旧い暗号鍵でＤｒ’＝Ｄｒ’（ｎ）となって一致した場合ではカード読出／書込機６

は、乗車カード７が使用していた暗号鍵はその番号の旧い暗号鍵Ｋ（ｎ）と判断し、乗車カード７に対して、現在使用されている暗号鍵Ｋ（０）に更新するように、すなわち、暗号鍵記憶メモリ１１のポインタｎの暗号鍵を使用している乗車カード７に対して、ポインタ０の暗号鍵に更新するように暗号鍵更新コマンドを送出し（ステップｎ１９）、乗車カード７が使用する暗号鍵をＫ（０）に更新させてステップｎ２１以降の処理を行って乗車カード７が正当なものであると認証する。

【００７７】また、乗車カード７の暗号鍵の更新後、新しい暗号鍵を用いて再度認証を行うようにしても構わない。なお、読出／書込機６が保有する旧い暗号鍵のいずれの暗号鍵でも暗号文が一致しなかったときには、その乗車カード７は不正な乗車カード７と判断する（ステップｎ２０）。

【００７８】次に、カード発行機４の読出／書込機６による処理について説明する。

【００７９】カード発行機４では、図１０で示されているようにポーリング、レスポンス受信、相互認証ＯＫについて図８と同様である。図１０で相互認証が終了すると、暗号鍵書き換えコマンドを送信し、乗車カード７の暗号鍵を含むデータの書き換えの処理を行う（ステップｎ４）。その際、乗車カード７の暗号鍵記憶メモリ１１の複数の暗号鍵を、現在使用する暗号鍵と今後使用する予定の複数の暗号鍵に書き換える（ステップｎ５）。これによって、乗車カード７は、当初は、現在使用する暗号鍵を選択して使用し、以後は、更新コマンドによって使用する暗号鍵を順番に更新する。

【００８０】なお、乗車カードが、使用されたカードを回収して発行するのではなく、全く、新規に乗車カードを発行する場合には、相互認証を行うことなく、現在使用する暗号鍵と今後使用する予定の複数の暗号鍵を書き込めばよい。

【００８１】上述の実施の形態では、自動改札などの駅務システムに適用したけれども、本発明は、かかるシステムに限定されるものではなく、自動料金徴収システムあるいはその他のシステムにも適用されるものである。

【００８２】また、上述の実施の形態では、非接触方式の通信に適用したけれども、本発明は、接触方式の通信にも適用され得る。

【００８３】

【発明の効果】以上のように本発明によれば次の効果を得られる。

【００８４】請求項１の本発明の記憶媒体によれば、読出／書込機との間の暗号処理において、複数の暗号鍵のいずれかを用いて暗号処理を行うので、共通暗号鍵方式のように一つの共通暗号鍵が解読されてもシステム全体のセキュリティ性が損なわれることがなく、また、使用する暗号鍵も読出／書込機からのコマンドによって必要に応じて更新されるので、ランダムにすべての暗号鍵を用いる従来例のように、すべての暗号鍵が傍受されて解読される虞れが低く、セキュリティ性が向上する。

【００８５】請求項２の本発明の記憶媒体によれば、複数の暗号鍵の少なくとも一部の暗号鍵を読出／書込機から書き換えることができるので、記憶されている複数の暗号鍵が更新によってすべて使用されてしまうまでに、新たな暗号鍵に書き換えることができ、これによって、永続的に新しい暗号鍵への更新が可能となり、セキュリティ性を永続的に確保できる。

【００８６】請求項３の本発明の読出／書込機によれば、記憶媒体が使用している暗号鍵が、過去に使用された暗号鍵であるか否かを判断し、読出／書込機で過去に使用されている暗号鍵であるときには、記憶媒体に更新コマンドを送出して記憶媒体が使用する暗号鍵を更新することができるので、記憶媒体の暗号鍵を、読出／書込機が現在使用している最新の暗号鍵に一致させることができる。したがって、記憶媒体が使用する暗号鍵を変更するために、記憶媒体を回収して暗号鍵を一斉に変更するといった困難な作業を行う必要がなく、記憶媒体が使用されて読出／書込機との間で通信を行うことにより、自動的に暗号鍵が変更されることになる。

【００８７】請求項４の本発明の読出／書込機によれば、上位機器からのコマンドによって使用する暗号鍵が変更されるので、必要に応じて、例えば、定期的あるいは現在使用している暗号鍵が解読される虞れがあるような時に、上位機器からのコマンドによって使用する暗号鍵を新しい暗号鍵に変更できることになり、セキュリティ性を確保でき、さらに、請求項３の作用によって、記憶媒体が使用する暗号鍵もその変更された暗号鍵に一致させることができる。

【００８８】請求項５の本発明の読出／書込機によれば、記憶媒体が記憶している複数の暗号鍵の少なくとも一部の暗号鍵を書き換えるので、記憶媒体の暗号鍵が順次更新されて記憶されている全ての暗号鍵が使用されてしまうまでに、新たな複数の暗号鍵に書き換えることができ、これによって、永続的に新しい暗号鍵への更新が可能となり、セキュリティ性を永続的に確保できる。

【００８９】請求項６の本発明のカードシステムによれば、カードと読出／書込機との暗号鍵が一致しなくても、カードの暗号鍵が、読出／書込機で過去に使用した暗号鍵であれば、カードの暗号鍵が更新されて読出／書込機の暗号鍵に一致するので、相互認証が可能となる。しかも、記憶媒体をカードとしているので、自動料金収集システムなどの各種の用途に好適に実施できることになり、請求項１ないし５の作用効果を顕著に奏することができる。

【００９０】請求項７の本発明の暗号鍵使用方法によれば、読出／書込機は、記憶媒体からの暗号化データと作成した暗号化データとを比較することにより、記憶媒体の暗号鍵が、読出／書込機が使用している暗号鍵に一致

しているか否かを判断し、一致していないときには、記憶媒体の暗号鍵が、過去に使用した暗号鍵であるか否かを判断し、過去の暗号鍵であるときには、記憶媒体の暗号鍵を更新させるので、記憶媒体の暗号鍵と読出／書込機との暗号鍵を一致させることができる。

【００９１】また、記憶媒体および読出／書込機は、複数の暗号鍵を記憶しているので、一つの共通暗号鍵のみを記憶している共通暗号鍵方式のように共通暗号鍵が解読されてもシステム全体のセキュリティ性が損なわれることがなく、また、使用する暗号鍵も読出／書込機からのコマンドによって必要に応じて更新されるので、ランダムにすべての暗号鍵を用いる従来例のように、すべての暗号鍵が傍受されて解読される虞れが低く、さらに、記憶媒体に記憶されている複数の暗号鍵を一斉に変更するといった必要もない。

【００９２】請求項８の本発明の駅務システムによれば、乗車カードと自動改札機の読出／書込機との間の暗号処理において、乗車カードおよび読出／書込機は、複数の暗号鍵を記憶しているので、一つの共通暗号鍵のみを記憶している共通暗号鍵方式のように共通暗号鍵が解読されてもシステム全体のセキュリティ性が損なわれることがなく、また、使用する暗号鍵も読出／書込機からのコマンドによって必要に応じて更新されるので、ランダムにすべての暗号鍵を用いる従来例のように、すべての暗号鍵が傍受されて解読される虞れが低く、さらに、乗車カードに記憶されている複数の暗号鍵を一斉に変更するといった必要もない。

【００９３】請求項９の本発明の駅務システムによれば、カード発行機は、乗車カードの発行時に、乗車カードに記憶されている複数の暗号鍵を書き換えるので、永続的に新しい暗号鍵への更新が可能となり、システムのセキュリティ性を永続的に確保できる。

【００９４】請求項１０の本発明のカード発行機によれば、回収した乗車カードを用いるのではなく、全く新規な乗車カードの発行時において、相互認証などを行うことなく、現在使用する暗号鍵および将来使用する予定の複数の暗号鍵を書き込むとともに、現在使用する暗号鍵を選択するよう設定して乗車カードを発行できる。

【図面の簡単な説明】

【図１】　本発明の実施形態に係るシステムの概略構成図である。

【図２】　自動改札機の斜視図である。

【図３】　乗車カードのブロック図である。

【図４】　乗車カードの暗号鍵記憶メモリの記憶内容を示す図である。

【図５】　読出／書込機のブロック図である。

【図６】　暗号鍵の使用期間を示す図である。

【図７】　読出／書込機の乗車カード用暗号鍵記憶メモリの記憶内容を示す図である。

【図８】　自動改札機の読出／書込機の動作説明に供するフローチャートである。

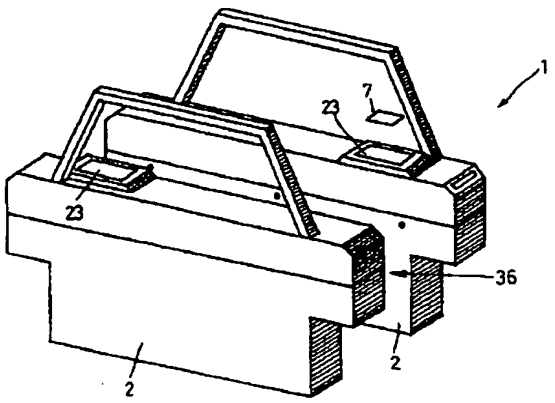
【図９】　相互認証の動作説明に供するフローチャートである。

【図１０】　カード発行機の読出／書込機の動作説明に供するフローチャートである。

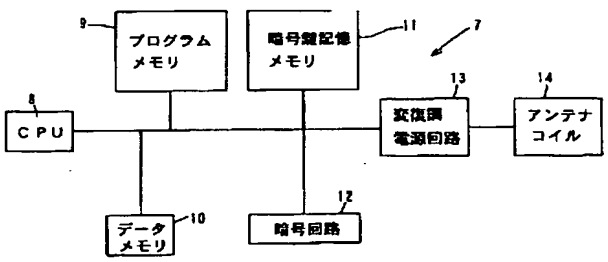
【符号の説明】

１	自動改札機
６	読出／書込機
７	乗車カード
８，１５	ＣＰＵ
１１	暗号鍵記憶メモリ
１４，２３	アンテナコイル
１９	乗車カード用暗号鍵記憶メモリ

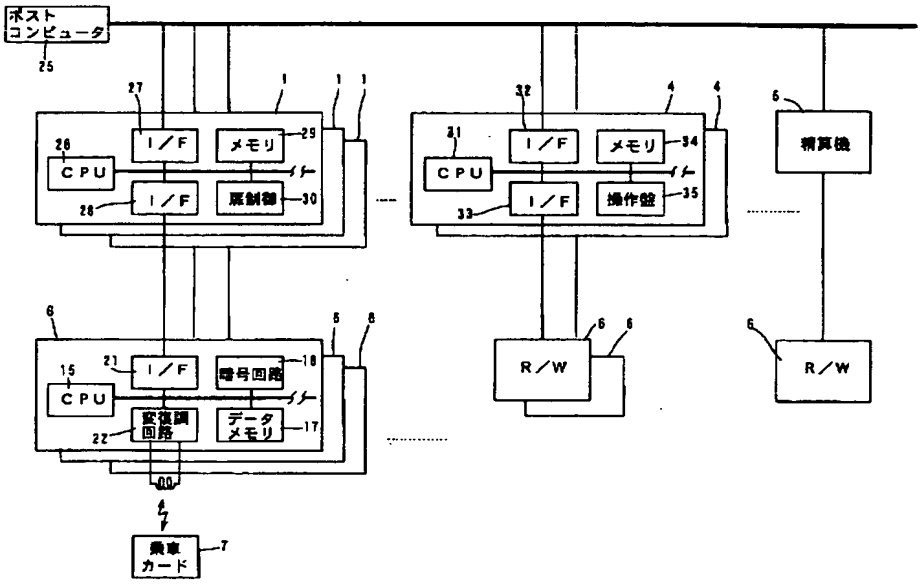
【図２】



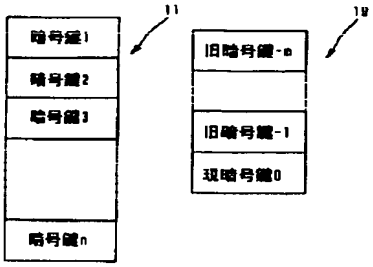
【図３】



【図１】

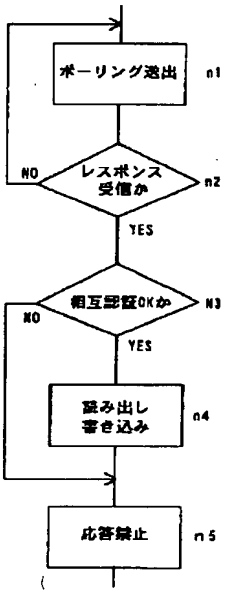


【図４】

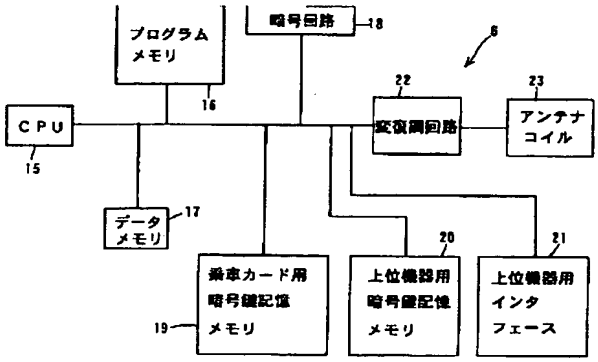


【図７】

【図８】



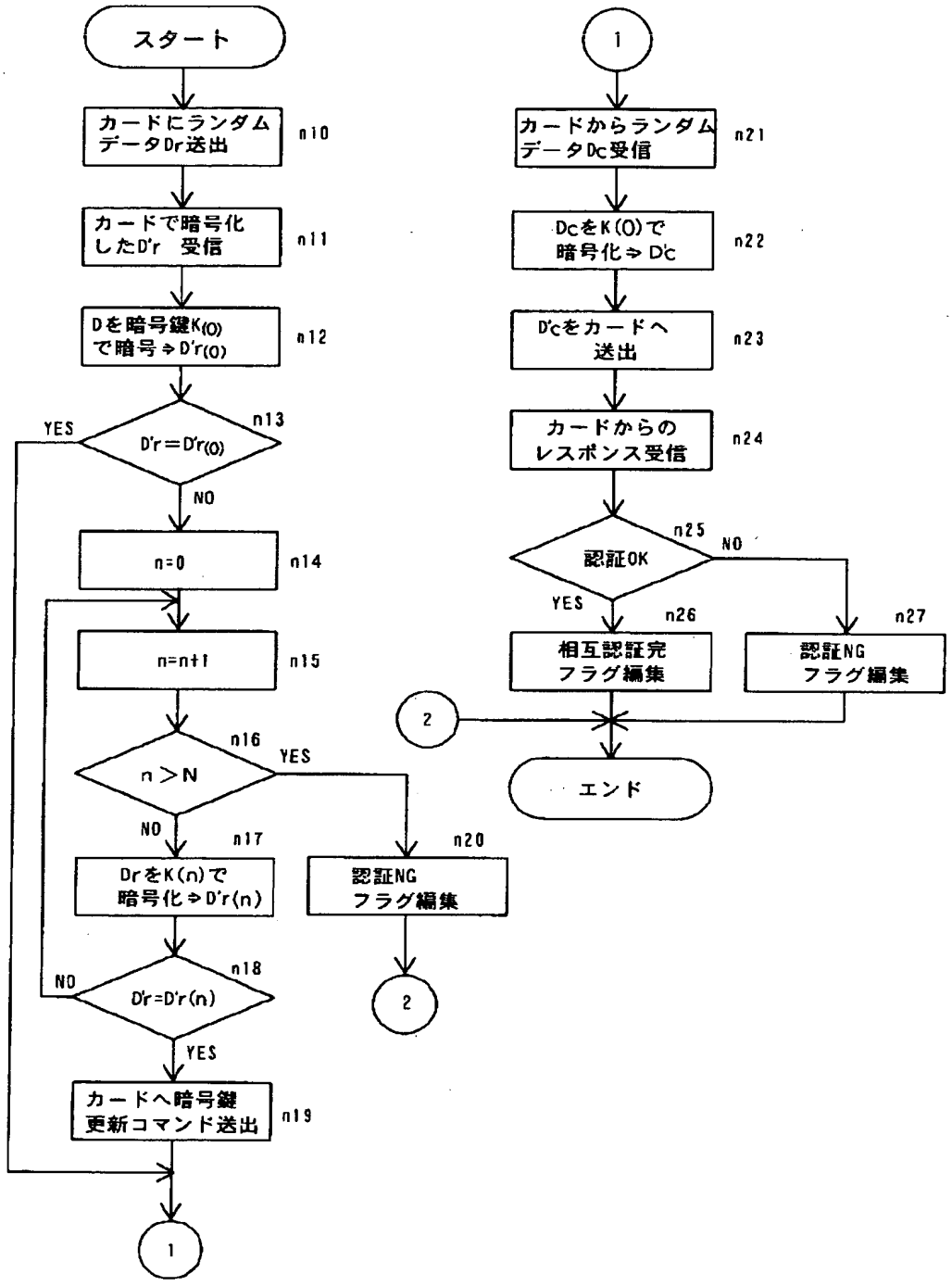
【図５】



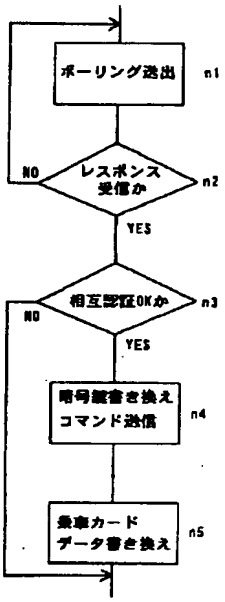
【図６】

暗号鍵	使用期間	状態
暗号鍵１	1998.01.01~ 1998.03.31	過去に使用
暗号鍵２	1998.04.01~ 1998.05.10	現在使用中
・ ・ ・		未使用
暗号鍵ｎ		未使用

【図９】


スタート
カードにランダムデータDr送出
n10
カードで暗号化したD'r　受信
n11
Dを暗号鍵K(0)で暗号⇒D'r(0)
n12
D'r＝D'r(0)
n13
YES
NO
n=0
n14
n=n+1
n15
n＞N
n16
YES
NO
DrをK(n)で暗号化⇒D'r(n)
n17
D'r=D'r(n)
n18
NO
YES
カードへ暗号鍵更新コマンド送出
n19
1
認証NG フラグ編集
n20
2
1
カードからランダムデータDc受信
n21
DcをK(0)で暗号化⇒D'c
n22
D'cをカードへ送出
n23
カードからのレスポンス受信
n24
認証OK
n25
NO
YES
相互認証完 フラグ編集
n26
認証NG フラグ編集
n27
2
エンド

【図１０】



フロントページの続き

(51) Int. Cl.⁷	識別記号	F I		テーマコード' (参考)
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７３Ｃ	